

Lattice Codes for Many-to-One Interference Channels With and Without Cognitive Messages

Jingge Zhu and Michael Gastpar, *Member, IEEE*

Abstract—A new achievable rate region is given for the Gaussian cognitive many-to-one interference channel. The proposed novel coding scheme is based on the compute-and-forward approach with lattice codes. Using the idea of decoding sums of codewords, our scheme improves considerably upon the conventional coding schemes which treat interference as noise or decode messages simultaneously. Our strategy also extends directly to the usual many-to-one interference channels without cognitive messages. Comparing to the usual compute-and-forward scheme where a fixed lattice is used for the code construction, the novel scheme employs scaled lattices and also encompasses key ingredients of the existing schemes for the cognitive interference channel. With this new component, our scheme achieves a larger rate region in general. For some symmetric channel settings, new constant gap or capacity results are established, which are independent of the number of users in the system.

I. INTRODUCTION

Recently, with growing requests on high data rate and increasing numbers of intelligent communication devices, the concept of *cognitive radio* has been intensively studied to boost spectral efficiency. As one of its information-theoretic abstractions, a model of the cognitive radio channel of two users was proposed and analyzed in [1], [2], [3]. In this model, the cognitive user is assumed to know the message of the primary user non-causally before transmissions take place. The capacity region of this channel with additive white Gaussian noise is known for most of the parameter region, see for example [4] for an overview of the results.

In this work we extend this cognitive radio channel model to include many cognitive users. We consider the simple many-to-one interference scenario with K cognitive users illustrated in Figure 1. The message W_0 (also called the *cognitive message*) of the primary user is given to all other K users, who could help the transmission of the primary user.

Existing coding schemes for the cognitive interference channel exploit the usefulness of cognitive messages. For the case $K = 1$, i.e., a single cognitive user, the strategy consists in letting the cognitive user spend part of its resources to help the

transmission of this message to the primary receiver. At the same time, this also appears as interference at the cognitive receiver. But dirty-paper coding can be used at the cognitive transmitter to cancel (part of) this interference. A new challenge arises when there are many cognitive users. The primary user now benefits from the help of all cognitive users, but at the same time suffers from their collective interference because cognitive users are also transmitting their own messages. This inherent tension is more pronounced when the channels from cognitive transmitters to the primary receiver are strong. In the existing coding scheme, the interference from cognitive users is either decoded or treated as noise at the primary receiver. As we will show later, direct extensions of these strategies to the many-to-one channel have significant shortcomings, especially when the interference is relatively strong.

The main contribution of this paper is a novel coding strategy for the cognitive interference network based on lattice codes. This scheme is based on the compute-and-forward approach ([5] [6]). It deals with interference in a beneficial fashion, enabling some degree of reconciliation between the competing factors mentioned above. While most of the compute-and-forward work considers a fixed lattice to be used at each transmitter, the strategy developed here employs scaled lattices. In general it achieves larger rates than using fixed lattices and permits us to derive constant gap and capacity results. We can also observe that the novel coding strategy encompasses several key ingredients of the existing coding schemes, such as rate splitting, dirty-paper coding and successive interference cancellation. The performance of the novel coding strategy is analyzed in detail. We show our scheme outperforms conventional coding schemes. The advantage is most notable in the case of strong interference from the cognitive users to the primary receiver. The proposed scheme applies naturally to the usual many-to-one interference channel, where the messages are not shared between users. Applying the proposed scheme to a symmetric channel setting, we can show that under certain channel conditions, the novel coding strategy is near-optimal (in a constant-gap sense) or optimal regardless of the number of cognitive users.

The basic idea of the proposed scheme is that instead of decoding its message directly, the primary decoder first recovers enough linear combinations of messages and then extracts its intended message. Lattice codes are well suited for this purpose because their linear structure matches the additivity of the channels. More specifically, when two codewords are superimposed additively, the resulting sum still lies in the lattice. To give an intuitive explanation as to why this property is beneficial in the interference channel, we note

Copyright (c) 2014 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

This work was supported in part by the European ERC Starting Grant 259530-ComCom. This paper was presented in part in IEEE International Symposium on Information Theory 2013, Istanbul, Turkey.

J. Zhu is with the School of Computer and Communication Sciences, Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland (e-mail: jingge.zhu@epfl.ch).

M. Gastpar is with the School of Computer and Communication Sciences, Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland and the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA, USA (e-mail: michael.gastpar@epfl.ch).

that as a general rule of thumb, the idea of interference alignment is needed in an interference network. However, using structured codes is a form of interference alignment. When the interfering codewords are summed up linearly by the channels, the interference signal (more precisely, the sumset of the interfering codewords) seen by the undesired receiver is much “smaller” when structured codes are used than when the codewords are chosen randomly. Hence the interference is “aligned” due to the linear structure of the codebook. This property gives powerful interference mitigation ability at the signal level.

Similar systems have been studied in the literature. For the case $K = 2$, the system under consideration is studied in [7]. A similar cognitive interference channel with so-called cumulative message sharing is also studied in [8] where each cognitive user has messages of multiple users. We note that those existing results have not exploited the possibility of using structured codes in cognitive interference networks. The many-to-one channel without cognitive message is studied in [9], where a similar idea of aligning interference based on lattice codes was used. We also point out that the method of compute-and-forward is versatile and beneficial in many network scenarios. For example it has been used in [10], [11] to study the Gaussian two-way relay channel, in [12] to study the K -user symmetric interference channel and in [13] to study the multiple-antenna system.

The paper is organized as follows. Section II introduces the system model and the problem statement. Section III extends the known coding schemes from the two-user cognitive channel to the many-to-one cognitive channel. A novel coding scheme is proposed in Section IV where we also discuss its features in details. In Section V we specialize our coding scheme to an interesting special case: the standard many-to-one interference channel without cognitive messages. We choose to present the cognitive channel first because it is more general and the results of the non-cognitive channel are absorbed in the former case.

We use the notation $[a : b]$ to denote a set of increasing integers $\{a, a+1, \dots, b\}$, \log to denote \log_2 and $\log^+(x)$, $[x]^+$ to denote the function $\max\{\log(x), 0\}$, $\max\{x, 0\}$, respectively. We use \bar{x} for $1 - x$ to lighten the notation at some places. We also adopt the convention that the sum $\sum_{i=m}^n x_i$ equals zero if $m > n$.

II. SYSTEM MODEL AND PROBLEM STATEMENT

We consider a multi-user channel consisting of $K + 1$ transmitter-receiver pairs as shown in Figure 1. The real-valued channel has the following vector representation:

$$\mathbf{y}_0 = \mathbf{x}_0 + \sum_{k=1}^K b_k \mathbf{x}_k + \mathbf{z}_0, \quad (1)$$

$$\mathbf{y}_k = h_k \mathbf{x}_k + \mathbf{z}_k, \quad k \in [1 : K], \quad (2)$$

where $\mathbf{x}_k, \mathbf{y}_k \in \mathbb{R}^n$ denote the channel input and output of the transmitter-receiver pair k , respectively. The noise $\mathbf{z}_k \in \mathbb{R}^n$ is assumed to be i.i.d. Gaussian with zero mean and unit variance for each entry. Let $b_k \geq 0$ denote the channel gain from Transmitter k to the Receiver 0 and h_k denote the

direct channel gain from Transmitter k to its corresponding receiver for $k \in [1 : K]$. We assume a unit channel gain for the first user without loss of generality. This system is sometimes referred to as the *many-to-one interference channel* (or *many-to-one channel* for simplicity), since only Receiver 0 experiences interference from other transmitters.

We assume that all users have the same power constraint, i.e., the channel input \mathbf{x}_k is subject to the power constraint

$$\mathbb{E}\{\|\mathbf{x}_k\|^2\} \leq nP, \quad k \in [1 : 0]. \quad (3)$$

Since channel gains are arbitrary, this assumption is without loss of generality. We also assume that all transmitters and receivers know their own channel coefficients; that is, b_k, h_k are known at Transmitter k , h_k is known at Receiver k , and $b_k, k \geq 1$ are known at Receiver 0.

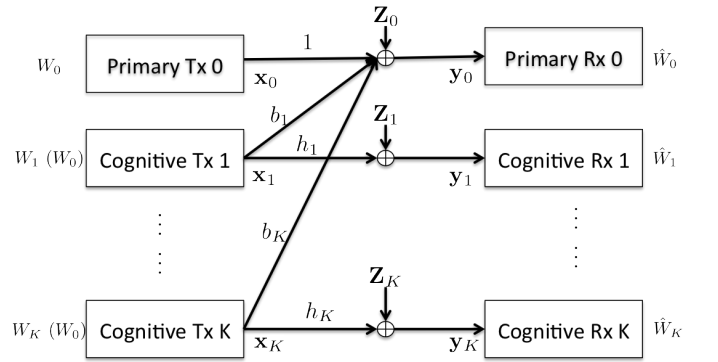


Fig. 1. A many-to-one interference channel. The message of the first user W_0 (called *cognitive message*) may or may not be present at other user's transmitter.

Now we introduce two variants of this channel according to different message configurations.

Definition 1 (Cognitive many-to-one channel): User 0 is called the primary user and User k a cognitive user (for $k \geq 1$). Each user has a message W_k from a set \mathcal{W}_k to send to its corresponding receiver. Furthermore, all the cognitive users also have access to the primary user's message W_0 (also called cognitive message).

Definition 2 (Non-cognitive many-to-one channel): Each user $k, k \in [0 : K]$ has a message W_k from a set \mathcal{W}_k to send to its corresponding receiver. The messages are not shared among users.

For the cognitive many-to-one channel, each transmitter has an encoder $\mathcal{E}_k : \mathcal{W}_k \rightarrow \mathbb{R}^n$ which maps the message to its channel input as

$$\mathbf{x}_0 = \mathcal{E}_0(W_0) \quad (4)$$

$$\mathbf{x}_k = \mathcal{E}_k(W_k, W_0), \quad k \in [1 : K]. \quad (5)$$

Each receiver has a decoder $\mathcal{D}_k : \mathbb{R}^n \rightarrow \mathcal{W}_k$ which estimates message \hat{W}_k from \mathbf{y}_k as

$$\hat{W}_k = \mathcal{D}_k(\mathbf{y}_k), \quad k \in [1 : K]. \quad (6)$$

The rate of each user is

$$R_k = \frac{1}{n} \log |\mathcal{W}_k| \quad (7)$$

under the average error probability requirement

$$\Pr \left(\bigcup_{k=0}^K \{\hat{W}_k \neq W_k\} \right) \rightarrow \epsilon \quad (8)$$

for any $\epsilon > 0$.

For the non-cognitive many-to-one channel, the encoder takes the form

$$\mathbf{x}_k = \mathcal{E}_k(W_k), \quad k \in [0 : K] \quad (9)$$

and other conditions are the same as in the cognitive channel.

As mentioned earlier, we find it convenient to first treat the general model—the cognitive many-to-one channel where we derive a novel coding scheme which outperforms conventional strategies. We will show that the coding scheme for the cognitive channel can be extended straightforwardly to the non-cognitive channel, which also gives new results for this channel.

III. EXTENSIONS OF CONVENTIONAL CODING SCHEMES

In this section we revisit existing coding schemes for the two-user cognitive interference channel and extend them to our cognitive many-to-one channel. The extensions are straightforward from the schemes proposed for the two-user cognitive channel in, for example, [1], [14] and [4]. Throughout the paper, many schemes can be parametrized by letting cognitive transmitters split their power. For each cognitive user, we introduce a power splitting parameter $0 \leq \lambda_k \leq 1$. For convenience, we also define the vector $\underline{\lambda} := \{\lambda_1, \dots, \lambda_K\}$.

In the first coding scheme, the cognitive users split the power and use part of it to transmit the message of the primary user. Luckily this part of the signal will not cause interference to the cognitive receiver since it can be completely canceled out using dirty-paper coding (DPC). We briefly describe the random coding argument for this coding scheme:

- **Primary encoder.** For each possible message W_0 , User 0 generates a codeword \mathbf{x}_0 with i.i.d. entries according to the Gaussian distribution $\mathcal{N}(0, P)$.
- **Cognitive encoders.** User k generates a sequence $\hat{\mathbf{x}}_k$ with i.i.d. entry according to the Gaussian distribution $\mathcal{N}(0, \bar{\lambda}_k P)$ for any given λ_k and form

$$\mathbf{u}_k = h_k \hat{\mathbf{x}}_k + \gamma h_k \sqrt{\lambda_k} \mathbf{x}_0 \quad (10)$$

with $\gamma = \bar{\lambda}_k h_k^2 P / (1 + \bar{\lambda}_k h_k^2 P)$, $k \geq 1$. The channel input is given by

$$\mathbf{x}_k = \sqrt{\lambda_k} \mathbf{x}_0 + \hat{\mathbf{x}}_k, \quad k \in [1 : K]. \quad (11)$$

- **Primary decoder.** Decoder 0 decodes \mathbf{x}_0 from \mathbf{y}_0 using typicality decoding.
- **Cognitive decoders.** Decoder k ($k \geq 1$) decodes \mathbf{u}_k from \mathbf{y}_k using typicality decoding.

This coding scheme gives the following achievable rate region.

Proposition 1 (DPC): For the cognitive many-to-one channel, the above dirty paper coding scheme achieves the rate

region:

$$R_0 \leq \frac{1}{2} \log \left(1 + \frac{(\sqrt{P} + \sum_{k \geq 1} b_k \sqrt{\lambda_k P})^2}{\sum_{k \geq 1} b_k^2 \bar{\lambda}_k P + 1} \right) \quad (12)$$

$$R_k \leq \frac{1}{2} \log (1 + \bar{\lambda}_k h_k^2 P), \quad k \in [1 : K] \quad (13)$$

for any power-splitting parameter $\underline{\lambda}$.

It is worth noting that this scheme achieves the capacity in the two-user case ($K = 1$) when $|b_1| \leq 1$, see [14, Theorem 3.7] for example.

Another coding scheme which performs well in the two-user case when $|b_1| > 1$, is to let the primary user decode the message of the cognitive user as well [4]. We extend this scheme by enabling *simultaneous nonunique decoding* (SND) [15, Ch. 6] at the primary decoder. SND improves the cognitive rates over uniquely decoding the messages $W_k, k \geq 1$ at primary decoder. We briefly describe the random coding argument for this coding scheme.

- **Primary encoder.** For each possible message W_0 , User 0 generates a codeword \mathbf{x}_0 with i.i.d. entries according to the distribution $\mathcal{N}(0, P)$.
- **Cognitive encoders.** Given the power splitting parameters λ_k , user k generates $\hat{\mathbf{x}}_k$ with i.i.d. entry according to the distribution $\mathcal{N}(0, \bar{\lambda}_k P)$ for its message $W_k, k \geq 1$. The channel input is given by

$$\mathbf{x}_k = \sqrt{\lambda_k} \mathbf{x}_0 + \hat{\mathbf{x}}_k \quad (14)$$

- **Primary decoder.** Decoder 0 simultaneously decodes $\mathbf{x}_0, \hat{\mathbf{x}}_1, \dots, \hat{\mathbf{x}}_K$ from \mathbf{y}_1 using typicality decoding. More precisely, let $T^{(n)}(Y_0, X_0, \hat{X}_1, \dots, \hat{X}_K)$ denotes the set of n -length typical sequences (see, for example [15, Ch. 2]) of the joint distribution $(\prod_{i=1}^K P_{\hat{X}_i}) P_{X_0} P_{Y_0|X_0, \dots, \hat{X}_K}$. The primary decoder decodes its message \mathbf{x}_0 such that

$$(\mathbf{x}_0, \hat{\mathbf{x}}_1, \dots, \hat{\mathbf{x}}_K) \in T^{(n)}(Y_0, X_0, \hat{X}_1, \dots, \hat{X}_K) \quad (15)$$

for a unique \mathbf{x}_0 and *some* $\hat{\mathbf{x}}_k, k \geq 1$.

- **Cognitive decoders.** Decoder k decodes $\hat{\mathbf{x}}_k$ from \mathbf{y}_k for $k \geq 1$.

We have the following achievable rate region for the above coding scheme.

Proposition 2 (SND at Rx 0): For the cognitive many-to-one channel, the above simultaneous nonunique decoding scheme achieves the rate region:

$$\begin{aligned} R_0 &\leq \frac{1}{2} \log \left(1 + \left(\sqrt{P} + \sum_{k \geq 1} b_k \sqrt{\lambda_k P} \right)^2 \right) \\ R_0 + \sum_{k \in \mathcal{J}} R_k &\leq \frac{1}{2} \log \left(1 + \sum_{k \in \mathcal{J}} b_k^2 \bar{\lambda}_k P \right. \\ &\quad \left. + \left(\sqrt{P} + \sum_{k \geq 1} b_k \sqrt{\lambda_k P} \right)^2 \right) \\ R_k &\leq \frac{1}{2} \log \left(1 + \frac{\bar{\lambda}_k h_k^2 P_k}{1 + \lambda_k h_k^2 P_k} \right) \end{aligned}$$

for any power-splitting parameter $\underline{\lambda}$ and every subset $\mathcal{J} \subseteq [1 : K]$.

We point out that if instead of using simultaneous nonunique decoding at the primary decoder but require it to decode all messages of the cognitive users $W_k, k \geq 1$, we would have the extra constraints

$$\sum_{k \in \mathcal{J}} R_k \leq \frac{1}{2} \log \left(1 + \sum_{k \in \mathcal{J}} b_k^2 \bar{\lambda}_k P \right) \quad (16)$$

for every subset $\mathcal{J} \subseteq [1 : K]$, which may further reduce the achievable rate region.

For the two-user case ($K = 1$), the above scheme achieves the capacity when $|b_1| \geq \sqrt{1 + P + P^2} + P$, see [4, Theorem V.2] for example.

We can further extend the above coding schemes by combining both dirty paper coding and SND at Rx 0, as it is done in [4, Theorem IV.1]. However this results in a very cumbersome rate expression in this system but gives little insight to the problem. On the other hand, we will show in the sequel that our proposed scheme combines the ideas in the above two schemes in a unified framework.

IV. A LATTICE CODES BASED SCHEME FOR COGNITIVE MANY-TO-ONE CHANNELS

In this section we provide a novel coding scheme for the cognitive many-to-one channels based on a modified compute-and-forward scheme. The key idea of this approach is that instead of decoding the desired codeword directly at the primary receiver, it is more beneficial to first recover several integer combinations of the codewords and then solve for the desired message. We first briefly introduce the nested lattice codes used for this coding scheme and then describe how to adapt the compute-and-forward technique to our problem.

A. Nested Lattice Codes

A lattice Λ is a discrete subgroup of \mathbb{R}^n with the property that if $\mathbf{t}_1, \mathbf{t}_2 \in \Lambda$, then $\mathbf{t}_1 + \mathbf{t}_2 \in \Lambda$. The details about lattice and lattice codes can be found, for example, in [16] [17]. The lattice quantizer $Q_\Lambda : \mathbb{R}^n \rightarrow \Lambda$ is defined as as:

$$Q_\Lambda(\mathbf{x}) = \operatorname{argmin}_{\mathbf{t} \in \Lambda} \|\mathbf{t} - \mathbf{x}\| \quad (17)$$

The fundamental Voronoi region of a lattice Λ is defined to be

$$\mathcal{V} := \{\mathbf{x} \in \mathbb{R}^n : Q_\Lambda(\mathbf{x}) = \mathbf{0}\} \quad (18)$$

The modulo operation gives the quantization error with respect to the lattice:

$$[\mathbf{x}] \bmod \Lambda = \mathbf{x} - Q_\Lambda(\mathbf{x}) \quad (19)$$

Two lattices Λ and Λ' are said to be nested if $\Lambda' \subseteq \Lambda$. A nested lattice code \mathcal{C} can be constructed using the coarse Λ' for *shaping* and the fine lattice Λ as codewords:

$$\mathcal{C} := \{\mathbf{t} \in \mathbb{R}^n : \mathbf{t} \in \Lambda \cap \mathcal{V}'\} \quad (20)$$

where \mathcal{V}' is the Voronoi region of Λ' . The *second moment* of the lattice Λ' per dimension is defined to be

$$\sigma^2(\Lambda') = \frac{1}{n \operatorname{Vol}(\mathcal{V}')} \int_{\mathcal{V}'} \|\mathbf{x}\|^2 d\mathbf{x} \quad (21)$$

which is also the average power of code \mathcal{C} defined in (20) if the codewords \mathbf{t} are uniformly distributed in \mathcal{V}' .

The following two definitions are important for the lattice code construction considered here.

Definition 3 (Good for AWGN channel): Let \mathbf{z} be a length- n vector with i.i.d. Gaussian component $\mathcal{N}(0, \sigma_z^2)$. A sequence of n -dimensional lattices $\Lambda^{(n)}$ with its Voronoi region $\mathcal{V}^{(n)}$ is said to be good for AWGN channel if

$$\Pr(\mathbf{z} \notin \mathcal{V}^{(n)}) \leq e^{-nE_p(\mu)} \quad (22)$$

where

$$\mu = \frac{(\operatorname{Vol}(\mathcal{V}^{(n)}))^{2/n}}{2\pi e \sigma_z^2} \quad (23)$$

is the volume-to-noise ratio and $E_p(\mu)$ is the Poltyrev exponent [18] which is positive for $\mu > 1$.

Definition 4 (Good for quantization): A sequence of n -dimensional lattices $\Lambda^{(n)}$ is said to be good for quantization if

$$\lim_{n \rightarrow \infty} \frac{\sigma^2(\Lambda^{(n)})}{(\operatorname{Vol}(\mathcal{V}^{(n)}))^{2/n}} = \frac{1}{2\pi e} \quad (24)$$

with $\sigma^2(\Lambda^{(n)})$ denoting the second moment of the lattice $\Lambda^{(n)}$ defined in (21). Notice the quantity on the LHS approaches the limit from above.

Erez and Zamir [17] have shown that there exist nested lattice codes where the fine lattice and the coarse lattice are both good for AWGN channel and good for quantization. Nam et al. [19, Theorem 2] extend the results to the case when there are multiple nested lattice codes.

Now we construct the nested lattice codes for our problem. Let $\underline{\beta} := \{\beta_0, \dots, \beta_K\}$ denotes a set of positive numbers. For each user, we choose a lattice Λ_k which is good for AWGN channel. These $K+1$ fine lattices will form a nested lattice chain [19] according to a certain order which will be determined later. We let Λ_c denote the coarsest lattice among them, i.e., $\Lambda_c \subseteq \Lambda_k$ for all $k \in [0 : K]$. As shown in [19, Thm. 2], we can also find another $K+1$ simultaneously good nested lattices such that $\Lambda_k^s \subseteq \Lambda_c$ for all $k \in [0 : K]$ whose second moments satisfy

$$\sigma_0^2 := \sigma^2(\Lambda_0^s) = \beta_0^2 P \quad (25a)$$

$$\sigma_k^2 := \sigma^2(\Lambda_k^s) = (1 - \lambda_k) \beta_k^2 P, \quad k \in [1 : K] \quad (25b)$$

with given power-splitting parameters $\underline{\lambda}$. Introducing the scaling coefficients $\underline{\beta}$ enables us to flexibly balance the rates of different users and utilize the channel state information in a natural way. This point is made clear in the next section when we describe the coding scheme.

The codebook for user k is constructed as

$$\mathcal{C}_k := \{\mathbf{t}_k \in \mathbb{R}^n : \mathbf{t}_k \in \Lambda_k \cap \mathcal{V}_k^s\}, \quad k \in [0 : K] \quad (26)$$

where \mathcal{V}_k^s denotes the Voronoi region of the *shaping lattice* Λ_k^s used to enforce the power constraints. With this lattice code, the message rate of user k is also given by

$$R_k = \frac{1}{n} \log \frac{\operatorname{Vol}(\mathcal{V}_k^s)}{\operatorname{Vol}(\mathcal{V}_k)} \quad (27)$$

with \mathcal{V}_k denoting the Voronoi region of the fine lattice Λ_k .

B. Main Results

Equipped with the nested lattice codes constructed above, we are ready to specify the coding scheme. Each cognitive user splits its power and uses one part to help the primary receiver. Messages $W_k \in \mathcal{W}_k$ of user k are mapped surjectively to lattice points $\mathbf{t}_k \in \mathcal{C}_k$ for all k .

Let $\underline{\gamma} = \{\gamma_1, \dots, \gamma_K\}$ be K real numbers to be determined later. Given all messages W_k and their corresponding lattice points \mathbf{t}_k , transmitters form

$$\mathbf{x}_0 = \left\lfloor \frac{\mathbf{t}_0}{\beta_0} + \mathbf{d}_0 \right\rfloor \bmod \Lambda_0^s / \beta_0 \quad (28a)$$

$$\hat{\mathbf{x}}_k = \left\lfloor \frac{\mathbf{t}_k}{\beta_k} + \mathbf{d}_k - \frac{\gamma_k \mathbf{x}_0}{\beta_k} \right\rfloor \bmod \Lambda_k^s / \beta_k, k \in [1 : K] \quad (28b)$$

where \mathbf{d}_k (called *dither*) is a random vector independent of \mathbf{t}_k and uniformly distributed in $\mathcal{V}_k^s / \beta_k$. It follows that \mathbf{x}_0 is also uniformly distributed in $\mathcal{V}_0^s / \beta_0$ hence has average power $\beta_0^2 P / \beta_0^2 = P$ and is independent from \mathbf{t}_0 [17, Lemma 1]. Similarly $\hat{\mathbf{x}}_k$ has average power $\bar{\lambda}_k P$ and is independent from \mathbf{t}_k for all $k \geq 1$.

Although \mathbf{x}_0 will act as interference at cognitive receivers, it is possible to cancel its effect at the receivers since it is known to cognitive transmitters. The dirty-paper coding idea in the previous section can also be implemented within the framework of lattice codes, see for example [20]. The parameters $\underline{\gamma}$ are used to cancel \mathbf{x}_0 partially or completely at the cognitive receivers.

The channel input for the primary transmitter is \mathbf{x}_0 defined above and the channel input for each cognitive transmitter is

$$\mathbf{x}_k = \sqrt{\lambda_k} \mathbf{x}_0 + \hat{\mathbf{x}}_k, \quad k \in [1 : K]. \quad (29)$$

Notice that $\mathbb{E}\{\|\mathbf{x}_k\|^2\}/n = \lambda_k P + \bar{\lambda}_k P = P$ hence power constraints are satisfied for all cognitive users.

We first give an informal description of the coding scheme and then present the main theorem. Let $\mathbf{a} := [a_0, \dots, a_K] \in \mathbb{Z}^{K+1}$ be a vector of integers. We shall show that the integer sum of the lattice codewords $\sum_{k \geq 0} a_k \mathbf{t}_k$ can be decoded reliably at the primary user for certain rates R_k . After this, we continue decoding further integer sums with judiciously chosen coefficients and solve for the desired codeword using these sums at the end. An important observation (also made in [5] and [21]) is that the integer sums we have already decoded can be used to decode the subsequent integer sums. We now point out the new ingredients in our proposed scheme compared to the existing successive compute-and-forward schemes as in [21] and [5]. Firstly the scaling parameters introduced in (25) allow users to adjust their rates according to the channel gains and generally achieve larger rate regions. They will also be important for deriving constant gap and capacity results for the non-cognitive channel in Section V-A. Secondly as the cognitive message acts as interference at cognitive receivers, using dirty-paper coding against the cognitive message in general improves the cognitive rates. But its implementation within successive compute-and-forward framework is not straightforward and requires careful treatment, as shown later in our analysis.

In general, let $L \in [1 : K+1]$ be the total number of integer sums¹ the primary user decodes and we represent the L sets of coefficients in the following *coefficient matrix*:

$$\mathbf{A} = \begin{pmatrix} a_0(1) & a_1(1) & a_2(1) & \dots & a_K(1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_0(L) & a_1(L) & a_2(L) & \dots & a_K(L) \end{pmatrix}, \quad (30)$$

where the ℓ -th row $\mathbf{a}(\ell) := [a_0(\ell), \dots, a_K(\ell)]$ represents the coefficients for the ℓ -th integer sum $\sum_k a_k(\ell) \mathbf{t}_k$. We will show all L integer sums can be decoded reliably if the rate of user k satisfies

$$R_k \leq \min_{\underline{\lambda}} r_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\lambda}, \underline{\beta}, \underline{\gamma}) \quad (31)$$

with

$$r_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\lambda}, \underline{\beta}, \underline{\gamma}) := \max_{\alpha_1, \dots, \alpha_{\ell} \in \mathbb{R}} \frac{1}{2} \log^+ \left(\frac{\sigma_k^2}{N_0(\ell)} \right). \quad (32)$$

The notation $\mathbf{a}_{\ell|1:\ell-1}$ emphasizes the fact that when the primary decoder decodes the ℓ -th sum with coefficients $\mathbf{a}(\ell)$, all previously decoded sums with coefficients $\mathbf{a}(1), \dots, \mathbf{a}(\ell-1)$ are used. In the expression above σ_k^2 is given in (25) and $N_0(\ell)$ is defined as

$$N_0(\ell) := \alpha_{\ell}^2 + \sum_{k \geq 1} \left(\alpha_{\ell} b_k - a_k(\ell) \beta_k - \sum_{j=1}^{\ell-1} \alpha_j a_k(j) \beta_k \right)^2 \bar{\lambda}_k P \\ + \left(\alpha_{\ell} b_0 - a_0(\ell) \beta_0 - \sum_{j=1}^{\ell-1} \alpha_j a_0(j) \beta_0 - g(\ell) \right)^2 P \quad (33)$$

with

$$b_0 := 1 + \sum_{k \geq 1} b_k \sqrt{\lambda_k} \quad (34)$$

$$g(\ell) := \sum_{k \geq 1} \left(\sum_{j=1}^{\ell-1} \alpha_j a_k(j) + a_k(\ell) \right) \gamma_k. \quad (35)$$

For any matrix $\mathbf{A} \in \mathbb{F}_p^{L \times (K+1)}$, let $\mathbf{A}' \in \mathbb{F}_p^{L \times K}$ denote the matrix \mathbf{A} without the first column. We define a set of matrices as

$$\mathcal{A}(L) := \{ \mathbf{A} \in \mathbb{F}_p^{L \times (K+1)} : \text{rank}(\mathbf{A}) = m, \text{rank}(\mathbf{A}') = m-1 \\ \text{for some integer } m, 1 \leq m \leq L \}. \quad (36)$$

We will show that if the coefficients matrix \mathbf{A} of the L integer sums is in this set, the desired codeword \mathbf{t}_0 can be reconstructed at the primary decoder. For cognitive receivers, the decoding procedure is much simpler. They will decode the desired codewords directly using lattice decoding.

Now we state the main theorem of this section formally and the proof will be presented in the next section.

Theorem 1: For any given set of power-splitting parameters $\underline{\lambda}$, positive numbers $\underline{\beta}, \underline{\gamma}$ and any coefficient matrix $\mathbf{A} \in \mathcal{A}(L)$ defined in (36) with $L \in [1 : K+1]$, define $\mathcal{L}_k := \{\ell \in [1 : L] | a_k(\ell) \neq 0\}$. If $r_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\lambda}, \underline{\beta}, \underline{\gamma}) > 0$ for all $\ell \in \mathcal{L}_k$,

¹There is no need to decode more than $K+1$ sums since there are $K+1$ users in total.

$k \in [0 : K]$, then the following rate is achievable for the cognitive many-to-one interference channel

$$R_0 \leq \min_{\ell \in \mathcal{L}_0} r_0(\mathbf{a}_{\ell|1:\ell-1}, \underline{\lambda}, \underline{\beta}, \underline{\gamma}) \quad (37a)$$

$$R_k \leq \min \left\{ \min_{\ell \in \mathcal{L}_k} r_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\lambda}, \underline{\beta}, \underline{\gamma}), \max_{\nu_k \in \mathbb{R}} \frac{1}{2} \log^+ \frac{\sigma_k^2}{N_k(\gamma_k)} \right\} \text{ for } k \geq 1. \quad (37b)$$

The expressions $r_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\lambda}, \underline{\beta}, \underline{\gamma})$ and σ_k^2 are defined in (32) and (25) respectively, and $N_k(\gamma_k)$ is defined as

$$N_k(\gamma_k) := \nu_k^2 + (\nu_k h_k - \beta_k)^2 \bar{\lambda}_k P + (\nu_k \sqrt{\lambda_k} h_k - \gamma_k)^2 P \quad (38)$$

Several comments are made on the above theorem. We use $r_k(\mathbf{a}_{\ell|1:\ell-1})$ to denote $r_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\lambda}, \underline{\beta}, \underline{\gamma})$ for brevity.

- In our coding scheme the primary user may decode more than one integer sums. In general, decoding the ℓ -th sum gives a constraint on R_k :

$$R_k \leq r_k(\mathbf{a}_{\ell|1:\ell-1}). \quad (39)$$

However notice that if $a_k(\ell) = 0$, i.e., the codeword \mathbf{t}_k is not in the ℓ -th sum, then R_k does not have to be constrained by $r_k(\mathbf{a}_{\ell|1:\ell-1})$ since this decoding does not concern Tx k . This explains the minimization of ℓ over the set \mathcal{L}_k in (37a) and (37b): the set \mathcal{L}_k denotes all sums in which the codeword \mathbf{t}_k participates and R_k is determined by the minimum of $r_k(\mathbf{a}_{\ell|1:\ell-1})$ over ℓ in \mathcal{L}_k .

- Notice that $r_k(\mathbf{a}_{\ell|1:\ell-1})$ is not necessarily positive and a negative value means that the ℓ -th sum cannot be decoded reliably. The whole decoding procedure will succeed only if all sums can be decoded successfully. Hence in the theorem we require $r_k(\mathbf{a}_{\ell|1:\ell-1}) > 0$ for all $\ell \in \mathcal{L}_k$ to ensure that all sums can be decoded.
- The primary user can choose which integer sums to decode, hence can maximize the rate over the number of integer sums L and the coefficients matrix \mathbf{A} in the set $\mathcal{A}(L)$, which gives the best rate as:

$$R_k \leq \max_{L \in [1:K+1]} \max_{\mathbf{A} \in \mathcal{A}(L)} \min_{\ell \in \mathcal{L}_k} r_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\lambda}, \underline{\beta}, \underline{\gamma}).$$

The optimal \mathbf{A} is the same for all k . To see this, notice that the denominator inside the log of the expression $r_k(\mathbf{a}_{\ell|1:\ell-1})$ in (32) is the same for all k and the numerator depends only on k but does not involve the coefficient matrix \mathbf{A} , hence the maximizing \mathbf{A} will be the same for all k .

- In the expression of $r_k(\mathbf{a}_{\ell|1:\ell-1})$ in (32) we should optimize over ℓ parameters $\alpha_1, \dots, \alpha_\ell$. The reason for involving these scaling factors is that there are two sources for the effective noise $N_0(\ell)$ at the lattice decoding stage, one is the non-integer channel gain and the other is the additive Gaussian noise in the channel. These scaling factors are used to balance these two effects and find the best trade-off between them, see [5, Section III] for a detailed explanation. The optimal α_ℓ can be given

explicitly but the expressions are very complicated hence we will not state it here. We note that the expression $r_k(\mathbf{a}_1)$ with the optimized α_1 , $\beta_k = 1$ and $\gamma_k = 0$ is the computation rate of compute-and-forward in [5, Theorem 2].

- As mentioned in Section IV-A, the parameters $\underline{\beta}$ are used for controlling the rate of individual users. Unlike the original compute-and-forward coding scheme in [5] where the transmitted signal \mathbf{x}_k contains the lattice codeword \mathbf{t}_k in the fine lattice Λ , the transmitted signal here contains a scaled version of the lattice codeword \mathbf{t}_k/β_k . By choosing different β_k for different user k we can adjust the rate of the individual user and achieve a larger rate region in general. More information about this modified scheme can be found in [6] where it is applied to other scenarios where the compute-and-forward technique is beneficial.
- For the cognitive users, their rates are constrained both by their direct channel to the corresponding receiver, and by the decoding procedure at the primary user. The two terms in (37b) reflect these two constraints. The parameters $\underline{\gamma}$ are used to (partially) cancel the interference \mathbf{x}_0 at the cognitive receivers. For example if we set $\gamma_k = \nu_k \sqrt{\lambda_k} h_k$, the cognitive receiver k will not experience any interference caused by \mathbf{x}_0 . However this affects the computation rate at the primary user in a non-trivial way through $r_k(\mathbf{a}_{\ell|1:\ell-1})$ (cf. Equations (32) and (33)).

This proposed scheme can be viewed as an extension of the techniques used in the conventional schemes discussed in section III. First of all it includes the dirty-paper coding within the lattice codes framework and we can show the following lemma.

Lemma 1: The achievable rates in Proposition 1 can be recovered using Theorem 2 by decoding one trivial sum with the coefficient $\mathbf{a}(1) = [1, 0, \dots, 0]$.

Proof: For given power-splitting parameters $\underline{\lambda}$ we decode only one trivial sum at the primary user by choosing $\mathbf{a}(1)$ such that $a_0(1) = 1$ and $a_k(1) = 0$ for $k \geq 1$, which is the same as decoding \mathbf{t}_0 . First consider decoding at the primary user. Using the expression (32) we have $R_k \leq r_k(\mathbf{a}(1)) = \frac{1}{2} \log(\sigma_k^2/N_0(1))$ with $N_0(1) = \alpha_1^2 \left(1 + \sum_{k \geq 1} b_k^2 \bar{\lambda}_k P\right) + (\alpha_1 b_0 - \beta_0)^2 P$ and $g(1) = 0$ with this choice of $\mathbf{a}(1)$ for any $\underline{\gamma}$. After optimizing α_1 we have

$$R_0 \leq \frac{1}{2} \log \left(1 + \frac{b_0^2 P}{1 + \sum_{k \geq 1} b_k^2 \bar{\lambda}_k P} \right). \quad (40)$$

Notice that this decoding does not impose any constraint on R_k for $k \geq 1$.

Now we consider the decoding process at the cognitive users. Choosing $\gamma_k = \nu_k \sqrt{\lambda_k} h_k$ in (38) will give $N_k(\gamma_k) = \nu_k^2 + (\nu_k h_k - \beta_k)^2 \bar{\lambda}_k P$ and

$$\max_{\nu_k \in \mathbb{R}} \frac{1}{2} \log^+ \frac{\sigma_k^2}{N_k(\gamma_k)} = \frac{1}{2} \log(1 + h_k^2 \bar{\lambda}_k P) \quad (41)$$

with the optimal $\nu_k^* = \frac{\beta_k h_k \bar{\lambda}_k P}{\lambda_k h_k^2 P + 1}$. This proves the claim. ■

The proposed scheme can also be viewed as an extension of simultaneous nonunique decoding (Proposition 2). Indeed, as observed in [22], SND can be replaced by either performing the usual joint (unique) decoding to decode all messages or treating interference as noise. The former case corresponds to decoding $K + 1$ integer sums with a full rank coefficient matrix and the latter case corresponds to decoding just one integer sum with the coefficients of cognitive users' messages being zero. Obviously our scheme includes these two cases. As a generalization, the proposed scheme decodes just enough sums of codewords without decoding the individual messages. Unfortunately it is difficult to show analytically that the achievable rates in Proposition 2 can be recovered using Theorem 1, since it would require the primary receiver to decode several non-trivial sums and the achievable rates are not analytically tractable for general channel gains. However the numerical examples in Section IV-E will show that the proposed scheme generally performs better than the conventional schemes.

C. On the Optimal Coefficient Matrix \mathbf{A}

From Theorem 1 and its following comments we see that the main difficulty in evaluating the expression $r_k(\mathbf{a}_{\ell[1:\ell-1]})$ in (37a) and (37b) is the maximization over all possible integer coefficient matrices in the set $\mathcal{A}(L)$. This is an integer programming problem and is analytically intractable for a system with general channel gains b_1, \dots, b_K . In this section we give an explicit formulation of this problem and an example of the choice of the coefficient matrix.

The expression $r_k(\mathbf{a}_{\ell[1:\ell-1]})$ in (32) is not directly amenable to analysis because finding the optimal solutions for the parameters $\{\alpha_\ell\}$ in (33) is prohibitively complex. Now we give an alternative formulation of the problem. We write $N_0(\ell)$ from Eq. (33) in the form of (43). It can be further rewritten compactly as

$$N_0(\ell) = \alpha_\ell^2 + \left\| \alpha_\ell \mathbf{h} - \tilde{\mathbf{a}}_\ell - \sum_{j=1}^{\ell-1} \alpha_j \tilde{\mathbf{a}}_j \right\|^2 P \quad (42)$$

where we define $\mathbf{h}, \tilde{\mathbf{a}}_j \in \mathbb{R}^K$ for $j \in [1 : \ell]$ in (44).

We will reformulate the above expression in such a way that the optimal parameters $\{\alpha_j\}$ have simple expressions and the optimization problem on \mathbf{A} can be stated explicitly. This is shown in the following proposition.

Proposition 3: Given $\tilde{\mathbf{a}}_j, j \in [1 : \ell - 1]$ and \mathbf{h} in (44), define

$$\begin{aligned} \mathbf{u}_j &= \tilde{\mathbf{a}}_j - \sum_{i=1}^{j-1} \tilde{\mathbf{a}}_i|_{\mathbf{u}_i}, \quad j = 1, \dots, \ell - 1 \\ \mathbf{u}_\ell &= \mathbf{h} - \sum_{i=1}^{\ell-1} \mathbf{h}|_{\mathbf{u}_i} \end{aligned} \quad (45)$$

where $\mathbf{x}|_{\mathbf{u}_i} := \frac{\mathbf{x}^T \mathbf{u}_i}{\|\mathbf{u}_i\|^2} \mathbf{u}_i$ denotes the projection of a vector \mathbf{x} on \mathbf{u}_i . The problem of finding the optimal coefficient matrix \mathbf{A} maximizing $r_k(\mathbf{a}_{\ell[1:\ell-1]})$ in Theorem 1 can be equivalently

formulated as the following optimization problem

$$\min_{\substack{L \in [1:K+1] \\ \mathbf{A} \in \mathcal{A}(L)}} \max_{\ell \in \mathcal{L}_k} \left\| \mathbf{B}_\ell^{1/2} \mathbf{a}(\ell) \right\| \quad (46)$$

where $\mathbf{a}(\ell)$ is the coefficient vector of the ℓ -th integer sum. The set $\mathcal{A}(L)$ is defined in (36) and $\mathcal{L}_k := \{\ell \in [1 : L] | a_k(\ell) \neq 0\}$. The notation $\mathbf{B}_\ell^{1/2}$ denotes a matrix satisfying² $\mathbf{B}_\ell^{1/2} \mathbf{B}_\ell^{1/2} = \mathbf{B}_\ell$, where \mathbf{B}_ℓ is given by

$$\mathbf{B}_\ell := \mathbf{C} \left(\mathbf{I} - \sum_{i=1}^{\ell-1} \frac{\mathbf{u}_i \mathbf{u}_i^T}{\|\mathbf{u}_i\|^2} - \frac{(\mathbf{u}_\ell \mathbf{u}_\ell^T) P}{1 + P \|\mathbf{u}_\ell\|^2} \right) \mathbf{C}^T, \quad (47)$$

and the matrix \mathbf{C} is defined as

$$\mathbf{C} := \begin{pmatrix} \beta_0 & 0 & 0 & \dots & 0 \\ \gamma_1 & \beta_1 \sqrt{\lambda_1} & 0 & \dots & 0 \\ \gamma_2 & 0 & \beta_2 \sqrt{\lambda_2} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \gamma_K & 0 & 0 & \dots & \beta_K \sqrt{\lambda_K} \end{pmatrix}. \quad (48)$$

Proof: The proof is given in Appendix B. \blacksquare

The above proposition makes the optimization of \mathbf{A} explicit, although solving this problem is still a computationally expensive task. We should point out that this problem is related to the *shortest vector problem* (SVP) where one is to find the shortest non-zero vector in a lattice. In particular let $\mathbf{B} \in \mathbb{R}^{K \times K}$ be a matrix whose columns constitute one set of basis vectors of the lattice, the SVP can be written as

$$\min_{\mathbf{a} \in \mathbb{Z}^K, \mathbf{a} \neq \mathbf{0}} \|\mathbf{B}\mathbf{a}\|. \quad (49)$$

Our problem in Proposition 3 is more complicated than solving L shortest vector problems. Because the L matrices $\mathbf{B}_\ell^{1/2}$ are related through the optimal integer vectors $\mathbf{a}(\ell)$ in a nontrivial manner and the objective in our problem is to minimize the maximal vector length $\max_\ell \left\| \mathbf{B}_\ell^{1/2} \mathbf{a}(\ell) \right\|$ of the L lattices. Furthermore the vectors $\mathbf{a}(1), \dots, \mathbf{a}(\ell)$ should lie in the set $\mathcal{A}(L)$ and the number of sums L is also an optimization variable. A low complexity algorithm has been found to solve this instance of SVP for the compute-and-forward problem in simple cases, see [23].

Here we provide an example on the optimal number of sums we need to decode. Consider a many-to-one channel with three cognitive users. We assume $b_1 = 3.5$ and vary b_2 and b_3 in the range $[0, 6]$. We set the direct channel gains $h_k = 1$ and consider four different power constraints. Now the goal is to maximize the sum rate

$$\max_{\substack{L \in [1:4] \\ \mathbf{A} \in \mathcal{A}(L)}} \sum_{k=0}^4 \min_{\ell \in \mathcal{L}_k} r_k(\mathbf{a}_{1:\ell-1}, \underline{\lambda}, \underline{\beta}, \underline{\gamma}) \quad (50)$$

with respect to $L \in [1 : 4]$, $\mathbf{A} \in \mathcal{A}(L)$ and $\underline{\beta} \in \mathbb{R}^4$. For simplicity we assume $\lambda_k = \gamma_k = 0$ for $k \geq 1$. Here we search for all possible \mathbf{A} and are interested in the optimal L : the optimal number of sums that need to be decoded.

²It is shown that $N_0 = P \mathbf{a}(\ell)^T \mathbf{B}_\ell \mathbf{a}(\ell)$ hence \mathbf{B}_ℓ is positive semi-definite because $N_0 \geq 0$. This guarantees the existence of $\mathbf{B}_\ell^{1/2}$.

$$N_0(\ell) := \alpha_\ell^2 + \sum_{k \geq 1} \left(\alpha_\ell b_k \sqrt{\lambda_k} - a_k(\ell) \beta_k \sqrt{\lambda_k} - \sum_{j=1}^{\ell-1} \alpha_j a_k(j) \beta_k \sqrt{\lambda_k} \right)^2 P \\ + \left(\alpha_\ell b_0 - a_0(\ell) \beta_0 - \sum_{k \geq 1} a_k(\ell) \gamma_k - \sum_{j=1}^{\ell-1} \alpha_j \left(a_0(j) \beta_0 + \sum_{k \geq 1} a_k(j) \gamma_k \right) \right)^2 P. \quad (43)$$

$$\mathbf{h} = [b_0, b_1 \sqrt{\lambda_1}, \dots, b_K \sqrt{\lambda_K}] \\ \tilde{\mathbf{a}}_j = \left[a_0(j) \beta_0 + \sum_{k \geq 1} a_k(j) \gamma_k, a_1(j) \beta_1 \sqrt{\lambda_1}, \dots, a_K(j) \beta_K \sqrt{\lambda_K} \right], \quad j \in [1 : \ell]. \quad (44)$$

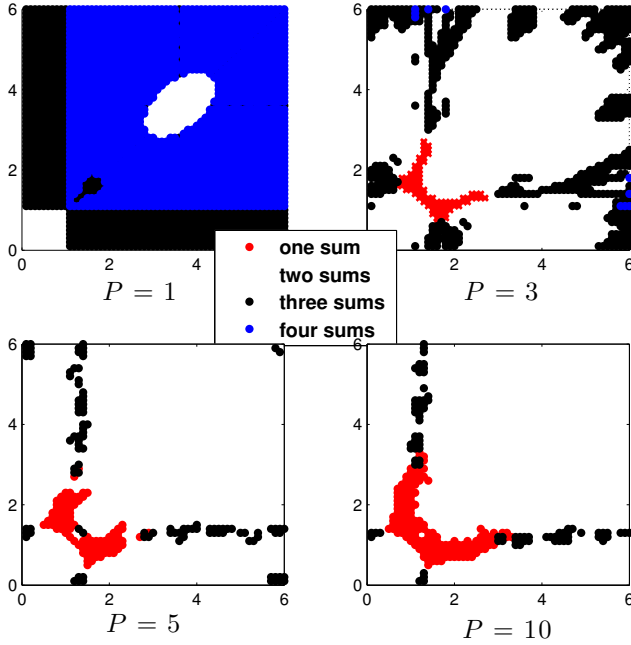


Fig. 2. We consider a many-to-one channel with three cognitive users and $b_1 = 3.5$. The horizontal and vertical axes are the range of b_2 and b_3 , respectively. The objective is to maximize the sum rate. The red, white, black and blue areas denote the region of different channel gains, in which the number of the best integer sums (the optimal L) is one, two, three and four respectively. Here the patterns are shown for four different power constraints.

The four plots in Figure 2 show the *optimal number of integer sums* that the primary user will decode for different power constraints where P equals 1, 3, 5 or 10. The red area denotes the channel gains where the optimal L equals 1, meaning we need only decode one sum to optimize the sum rate, and so on. Notice that the sign of the channel coefficients b_2, b_3 will not change the optimization problem hence the patterns should be symmetric over both horizontal and vertical axes. When power is small ($P = 1$) we need to decode more than two sums in most channel conditions. The patterns for P equals 3, 5 or 10 look similar but otherwise rather arbitrary—reflecting the complex nature of the solution to an integer programming problem. One observation from the plots

is that for P relatively large, with most channel conditions we only need to decode two sums and we do not decode four sums, which is equivalent to solving for all messages. This confirms the point we made in the previous section: the proposed scheme generalizes the conventional scheme such as Proposition 2 to decode just enough information for its purpose, but not more.

D. Proof of Theorem 1

In this section we provide a detailed proof for Theorem 1. We also discuss the choice of the fine lattices Λ_k introduced in IV-A. The encoding procedure has been discussed in section IV-B, now we consider the decoding procedure at the primary user. The received signal \mathbf{y}_0 at the primary decoder is

$$\mathbf{y}_0 = \mathbf{x}_0 + \sum_{k \geq 1} b_k \mathbf{x}_k + \mathbf{z}_0 \quad (51)$$

$$= (1 + \sum_{k \geq 1} b_k \sqrt{\lambda_k}) \mathbf{x}_0 + \sum_{k \geq 1} b_k \hat{\mathbf{x}}_k + \mathbf{z}_0 \quad (52)$$

$$= b_0 \mathbf{x}_0 + \sum_{k \geq 1} b_k \hat{\mathbf{x}}_k + \mathbf{z}_0 \quad (53)$$

where we define $b_0 := 1 + \sum_{k \geq 1} b_k \sqrt{\lambda_k}$.

Given a set of integers $\mathbf{a}(1) := \{a_k(1) \in \mathbb{Z}, k \in [0 : K]\}$ and some scalar $\alpha_1 \in \mathbb{R}$, the primary decoder can form the following:

$$\tilde{\mathbf{y}}_0^{(1)} = \alpha_1 \mathbf{y}_0 - \sum_{k \geq 0} a_k(1) \beta_k \mathbf{d}_k \\ = (\alpha_1 b_0 - a_0(1) \beta_0) \mathbf{x}_0 + \sum_{k \geq 1} (\alpha_1 b_k - a_k(1) \beta_k) \hat{\mathbf{x}}_k + \alpha_1 \mathbf{z}_0 \\ + \sum_{k \geq 1} a_k(1) \beta_k \hat{\mathbf{x}}_k + a_0(1) \beta_0 \mathbf{x}_0 - \sum_{k \geq 0} a_k(1) \beta_k \mathbf{d}_k.$$

Rewrite the last three terms in the above expression as

$$\begin{aligned}
& \sum_{k \geq 1} a_k(1) \beta_k \hat{\mathbf{x}}_k + a_0(1) \beta_0 \mathbf{x}_0 - \sum_{k \geq 0} a_k(1) \beta_k \mathbf{d}_k \\
& \stackrel{(b)}{=} \sum_{k \geq 1} a_k(1) \left(\beta_k \left(\frac{\mathbf{t}_k}{\beta_k} - \frac{\gamma_k \mathbf{x}_0}{\beta_k} \right) - \beta_k Q_{\Lambda_k^s} \left(\frac{\mathbf{t}_k}{\beta_k} + \mathbf{d}_k - \frac{\gamma_k \mathbf{x}_0}{\beta_k} \right) \right) \\
& \quad + a_0(1) \left(\beta_0 \mathbf{t}_0 - \beta_0 Q_{\Lambda_0^s} \left(\frac{\mathbf{t}_0}{\beta_0} + \mathbf{d}_0 \right) \right) \\
& \stackrel{(c)}{=} - \sum_{k \geq 1} a_k(1) \gamma_k \mathbf{x}_0 + a_0(1) (\mathbf{t}_0 - Q_{\Lambda_0^s} (\mathbf{t}_0 + \beta_0 \mathbf{d}_0)) \\
& \quad + \sum_{k \geq 1} a_k(1) (\mathbf{t}_k - Q_{\Lambda_k^s} (\mathbf{t}_k + \beta_k \mathbf{d}_k - \gamma_k \mathbf{x}_0)) \\
& \stackrel{(d)}{=} - \sum_{k \geq 1} a_k(1) \gamma_k \mathbf{x}_0 + \sum_{k \geq 0} a_k(1) \tilde{\mathbf{t}}_k. \tag{54}
\end{aligned}$$

In step (b) we used the definition of the signals \mathbf{x}_0 and $\hat{\mathbf{x}}_k$ from Eqn. (28b). Step (c) uses the identity $Q_{\Lambda}(\beta \mathbf{x}) = \beta Q_{\Lambda/\beta}(\mathbf{x})$ for any real number $\beta \neq 0$. In step (d) we define $\tilde{\mathbf{t}}_k$ for user k as

$$\tilde{\mathbf{t}}_0 := \mathbf{t}_0 - Q_{\Lambda_0^s}(\mathbf{t}_0 + \beta_0 \mathbf{d}_0) \tag{55}$$

$$\tilde{\mathbf{t}}_k := \mathbf{t}_k - Q_{\Lambda_k^s}(\mathbf{t}_k + \beta_k \mathbf{d}_k - \gamma_k \mathbf{x}_0) \quad k \in [1 : K]. \tag{56}$$

Define $g(1) := \sum_{k \geq 1} a_k(1) \gamma_k$ and substitute the expression (54) into $\tilde{\mathbf{y}}_0^{(1)}$ to get

$$\begin{aligned}
\tilde{\mathbf{y}}_0^{(1)} &= (\alpha_1 b_0 - a_0(1) \beta_0 - g(1)) \mathbf{x}_0 + \sum_{k \geq 1} (\alpha_1 b_k - a_k(1) \beta_k) \hat{\mathbf{x}}_k \\
&\quad + \alpha_1 \mathbf{z}_0 + \sum_{k \geq 0} a_k(1) \tilde{\mathbf{t}}_k \\
&= \tilde{\mathbf{z}}_0(1) + \sum_{k \geq 0} a_k(1) \tilde{\mathbf{t}}_k \tag{57}
\end{aligned}$$

where we define the equivalent noise $\tilde{\mathbf{z}}_0(1)$ at the primary receiver as:

$$\begin{aligned}
\tilde{\mathbf{z}}_0(1) &:= \alpha_1 \mathbf{z}_0 + (\alpha_1 b_0 - a_0(1) \beta_0 - g(1)) \mathbf{x}_0 \\
&\quad + \sum_{k \geq 1} (\alpha_1 b_k - a_k(1) \beta_k) \hat{\mathbf{x}}_k \tag{58}
\end{aligned}$$

where $b_0 := 1 + \sum_{k \geq 1} b_k \sqrt{\lambda_k}$.

Notice that we have $\tilde{\mathbf{t}}_k \in \Lambda_k$ since $\mathbf{t}_k \in \Lambda_k$ and $\Lambda_k^s \subseteq \Lambda_c$ due to the lattice code construction (recall that Λ_c denotes the coarsest lattice among all Λ_k for $k \in [0 : K]$). Furthermore because all Λ_k are chosen to form a nested lattice chain, the integer combination $\sum_{k \geq 0} a_k(1) \tilde{\mathbf{t}}_k$ also belongs to the finest lattice among all Λ_k with $a_k(1) \neq 0$. We denote this finest lattice as Λ_f , i.e., $\Lambda_k \subseteq \Lambda_f$ for all $k \in [0 : K]$ satisfying $a_k(1) \neq 0$. Furthermore, the equivalent noise $\tilde{\mathbf{z}}_0(1)$ is independent of the signal $\sum_{k \geq 0} a_k(1) \tilde{\mathbf{t}}_k$ thanks to the dithers \mathbf{d}_k .

The primary decoder performs *lattice decoding* to decode the integer sum $\sum_{k \geq 0} a_k(1) \tilde{\mathbf{t}}_k$ by quantizing $\tilde{\mathbf{y}}_0^{(1)}$ to its nearest neighbor in Λ_f . A decoding error occurs when $\tilde{\mathbf{y}}_0^{(1)}$ falls outside the Voronoi region around the lattice point $\sum_{k \geq 0} a_k(1) \tilde{\mathbf{t}}_k$. The probability of this event is equal to the probability that the equivalent noise $\tilde{\mathbf{z}}_0(1)$ leaves the Voronoi region of the finest lattice, i.e., $\Pr(\tilde{\mathbf{z}}_0(1) \notin \mathcal{V}_f)$ where \mathcal{V}_f

denotes the Voronoi region of Λ_f . The same as in the proof of [5, Theorem 5], the probability $\Pr(\tilde{\mathbf{z}}_0(1) \notin \mathcal{V}_f)$ goes to zero if the probability $\Pr(\mathbf{z}_0^*(1) \notin \mathcal{V}_f)$ goes to zero where $\mathbf{z}_0^*(1)$ is a zero-mean Gaussian vector with i.i.d entries whose variance equals the variance of the noise $\tilde{\mathbf{z}}_0(1)$:

$$\begin{aligned}
N_0(1) &= \alpha_1^2 + (\alpha_1 b_0 - a_0(1) \beta_0 - g(1))^2 P \\
&\quad + \sum_{k \geq 1} (\alpha_1 b_k - a_k(1) \beta_k)^2 \bar{\lambda}_k P.
\end{aligned}$$

By the AWGN goodness property (Definition 3) of Λ_f , the probability $\Pr(\mathbf{z}_0^*(1) \notin \mathcal{V}_f)$ goes to zero exponentially if

$$\frac{(\text{Vol}(\mathcal{V}_f))^{2/n}}{N_0(1)} > 2\pi e. \tag{59}$$

Since Λ_f is the finest lattice in the nested lattice chain formed by $\Lambda_k, k \in [0 : K]$ satisfying $a_k(1) \neq 0$, namely

$$\text{Vol}(\mathcal{V}_f) = \min_{k \in [0 : K], a_k(1) \neq 0} \text{Vol}(\mathcal{V}_k),$$

the inequality in (59) holds if it holds that

$$\frac{(\text{Vol}(\mathcal{V}_k))^{2/n}}{N_0(1)} > 2\pi e. \tag{60}$$

for all $k \in [0 : K]$ satisfying $a_k(1) \neq 0$. Hence using the rate expression

$$R_k = \frac{1}{n} \log \frac{\text{Vol}(\mathcal{V}_k^s)}{\text{Vol}(\mathcal{V}_k)} \tag{61}$$

we see the error probability goes to zero, or equivalently (59) holds, if

$$2^{2R_k} \leq \frac{(\text{Vol}(\mathcal{V}_k^s))^{2/n}}{2\pi e N_0(1)} \tag{62}$$

for all $k \in [0 : K]$ satisfying $a_k(1) \neq 0$. For Tx k with $a_k(1) = 0$, decoding this integer sum will not impose any constraint on the rate R_k .

Recalling the fact that Λ_k^s is good for quantization (Definition 4), we have

$$\frac{\sigma_k^2}{(\text{Vol}(\mathcal{V}_k^s))^{2/n}} < \frac{(1 + \delta)}{2\pi e} \tag{63}$$

for any $\delta > 0$. We conclude that lattice decoding will be successful if

$$R_k < r_k(\mathbf{a}_1, \underline{\lambda}, \underline{\beta}, \underline{\gamma}) := \frac{1}{2} \log \frac{\sigma_k^2}{N_0(1)} - \frac{1}{2} \log(1 + \delta) \tag{64}$$

that is

$$R_0 < \frac{1}{2} \log^+ \left(\frac{\beta_0^2 P}{\alpha_1^2 + P \|\alpha_1 \mathbf{h} - \tilde{\mathbf{a}}\|^2} \right) \tag{65a}$$

$$R_k < \frac{1}{2} \log^+ \left(\frac{(1 - \lambda_k) \beta_k^2 P}{\alpha_1^2 + P \|\alpha_1 \mathbf{h} - \tilde{\mathbf{a}}\|^2} \right) \quad k \in [1 : K] \tag{65b}$$

if we choose δ arbitrarily small and define

$$\mathbf{h} := [b_0, b_1 \sqrt{\lambda_1}, \dots, b_K \sqrt{\lambda_K}]$$

$$\tilde{\mathbf{a}} := [a_0(1) \beta_0 + g(1), a_1(1) \beta_1 \sqrt{\lambda_1}, \dots, a_K(1) \beta_K \sqrt{\lambda_K}].$$

Notice we can optimize over α_1 to maximize the above rates.

At this point, the primary user has successfully decoded one integer sum of the lattice points $\sum_{k \geq 0} a_k \tilde{\mathbf{t}}_k$. As mentioned earlier, we may continue decoding other integer sums with the help of this sum. The method of performing *successive compute-and-forward* in [21] is to first recover a linear combination of all transmitted signals $\tilde{\mathbf{x}}_k$ from the decoded integer sum and use it for subsequent decoding. Here we are not able to do this because the cognitive channel input $\hat{\mathbf{x}}_k$ contains \mathbf{x}_0 which is not known at Receiver 0. In order to proceed, we use the observation that if $\sum_{k \geq 0} a_k \tilde{\mathbf{t}}_k$ can be decoded reliably, then we know the equivalent noise $\tilde{\mathbf{z}}_0(1)$ and can use it for the subsequent decoding.

In general assume the primary user has decoded $\ell-1$ integer sums $\sum_k a_k(j) \mathbf{t}_k$, $j \in [1 : \ell-1]$, $\ell \geq 2$ with positive rates, and about to decode another integer sum with coefficients $\mathbf{a}(\ell)$. We show in Appendix A that with the previously known $\tilde{\mathbf{z}}_0(\ell-1)$ for $\ell \geq 2$, the primary decoder can form

$$\tilde{\mathbf{y}}_0^{(\ell)} = \tilde{\mathbf{z}}_0(\ell) + \sum_{k \geq 0} a_k(\ell) \tilde{\mathbf{t}}_k \quad (66)$$

with the equivalent noise $\tilde{\mathbf{z}}_0(\ell)$

$$\begin{aligned} \tilde{\mathbf{z}}_0(\ell) := & \alpha_\ell \mathbf{z}_0 + \sum_{k \geq 1} \left(\alpha_\ell b_k - a_k(\ell) \beta_k - \sum_{j=1}^{\ell-1} \alpha_j a_k(j) \beta_k \right) \hat{\mathbf{x}}_k \\ & + \left(\alpha_\ell b_0 - a_0(\ell) \beta_0 - \sum_{j=1}^{\ell-1} \alpha_j a_0(j) \beta_0 - g(\ell) \right) \mathbf{x}_0 \end{aligned} \quad (67)$$

where $g(\ell)$ is defined in (35) and the scaling factors $\alpha_1, \dots, \alpha_\ell$ are to be optimized.

In the same vein as we derived (64), using $\tilde{\mathbf{y}}_0^{(\ell)}$ we can decode the integer sums of the lattice codewords $\sum_{k \geq 0} a_k(\ell) \tilde{\mathbf{t}}_0$ reliably using lattice decoding if the fine lattice satisfy

$$\frac{(\text{Vol}(\mathcal{V}_k))^{2/n}}{N_0(\ell)} > 2\pi e \quad (68)$$

for k satisfying $a_k(\ell) \neq 0$ and we use $N_0(\ell)$ to denote the variance of the equivalent noise $\tilde{\mathbf{z}}_0(\ell)$ per dimension given in (33). Equivalently we require the rate R_k to be smaller than

$$r_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\lambda}, \underline{\beta}, \underline{\gamma}) := \max_{\alpha_1, \dots, \alpha_\ell \in \mathbb{R}} \frac{1}{2} \log^+ \left(\frac{\sigma_k^2}{N_0(\ell)} \right) \quad (69)$$

where σ_k^2 is given in (25). Thus we arrive at the same expression in (32) as claimed.

Recalling the definition of the set $\mathcal{A}(L)$ in (36), we now show that if the coefficient matrix \mathbf{A} is in this set, the term $\tilde{\mathbf{t}}_0$ can be solved using the L integer sums with coefficients $\mathbf{a}(1), \dots, \mathbf{a}(L)$.

For the case $\text{rank}(\mathbf{A}) = K+1$ the statement is trivial. For the case $\text{rank}(\mathbf{A}) = m \leq L < K+1$, we know that by performing Gaussian elimination on $\mathbf{A}' \in \mathbb{Z}^{L \times K}$ with rank $m-1$, we obtain a matrix whose last $L-m+1$ rows are zeros. Notice that $\mathbf{A} \in \mathbb{Z}^{L \times K+1}$ is a matrix formed by adding one more column in front of \mathbf{A}' . So if we perform exactly the same Gaussian elimination procedure on the matrix \mathbf{A} , there must be at least one row in the last $L-m+1$ row whose first entry is non-zero, since $\text{rank}(\mathbf{A}) = \text{rank}(\mathbf{A}') + 1$. This row

will give the value of $\tilde{\mathbf{t}}_0$. Finally the true codeword \mathbf{t}_0 can be recovered as

$$\mathbf{t}_0 = [\tilde{\mathbf{t}}_0] \bmod \Lambda_0^s. \quad (70)$$

Now we consider the decoding procedure at cognitive receivers, for whom it is just a point-to-point transmission problem over Gaussian channel using lattice codes. The cognitive user k processes its received signal for some ν_k as

$$\begin{aligned} \tilde{\mathbf{y}}_k &= \nu_k \mathbf{y}_k - \beta_k \mathbf{d}_k \\ &= \nu_k (\mathbf{z}_k + \sqrt{\lambda_k} h_k \mathbf{x}_0) + (\nu_k h_k - \beta_k) \hat{\mathbf{x}}_k + \beta_k \hat{\mathbf{x}}_k - \beta_k \mathbf{d}_k \\ &= \nu_k (\mathbf{z}_k + \sqrt{\lambda_k} h_k \mathbf{x}_0) + (\nu_k h_k - \beta_k) \hat{\mathbf{x}}_k - \beta_k \mathbf{d}_k \\ &\quad + Q_{\Lambda_k^s}(\mathbf{t}_k + \beta_k \mathbf{d}_k - \gamma_k \mathbf{x}_0) + \beta_k \left(\frac{\mathbf{t}_k}{\beta_k} + \mathbf{d}_k - \frac{\gamma_k}{\beta_k} \mathbf{x}_0 \right) \\ &= \tilde{\mathbf{z}}_k + \tilde{\mathbf{t}}_k. \end{aligned}$$

In the last step we define the equivalent noise as

$$\tilde{\mathbf{z}}_k := \nu_k \mathbf{z}_k + (\nu_k h_k - \beta_k) \hat{\mathbf{x}}_k + (\nu_k \sqrt{\lambda_k} h_k - \gamma_k) \mathbf{x}_0 \quad (71)$$

and $\tilde{\mathbf{t}}_k$ as in (56).

Using the same argument as before, we can show that the codeword $\tilde{\mathbf{t}}_k$ can be decoded reliably using lattice decoding if

$$\frac{(\text{Vol}(\mathcal{V}_k))^{2/n}}{N_k(\gamma_k)} > 2\pi e \quad (72)$$

for all $k \geq 1$ where $N_k(\gamma)$ is the variance of the equivalent noise $\tilde{\mathbf{z}}_k$ per dimension given in (38). Equivalently the cognitive rate R_k should satisfy

$$R_k < \max_{\nu_k} \frac{1}{2} \log \frac{\sigma_k^2}{N_k(\gamma_k)}. \quad (73)$$

Similarly we can obtain \mathbf{t}_k from $\tilde{\mathbf{t}}_k$ as $\mathbf{t}_k = [\tilde{\mathbf{t}}_k] \bmod \Lambda_k^s$. This completes the proof of Theorem 1.

We also determined how to choose the fine lattice Λ_k . Summarizing the requirements in (72) and (68) on Λ_k for successful decoding, the fine lattice Λ_0 of the primary user satisfies

$$(\text{Vol}(\mathcal{V}_0))^{2/n} > 2\pi e N_0(\ell) \quad (74)$$

for all ℓ where $a_0(\ell) \neq 0$ and the fine lattice Λ_k of the cognitive user k , $k \in [1 : K]$, satisfies

$$(\text{Vol}(\mathcal{V}_k))^{2/n} > \max\{2\pi e N_0(\ell), 2\pi e N_k(\gamma_k)\} \quad (75)$$

for all ℓ where $a_k(\ell) \neq 0$. As mentioned in Section IV-A, the fine lattices Λ_k are chosen to form a nested lattice chain. Now the order of this chain can be determined by the volumes of \mathcal{V}_k given above.

E. Symmetric Cognitive Many-to-One Channels

As we have seen in Section IV-C, it is in general difficult to describe the optimal coefficient matrix \mathbf{A} . However we can give a partial answer to this question if we focus on one simple class of many-to-one channels. In this section we consider a symmetric system with $b_k = b$ and $h_k = h$ for all $k \geq 1$ and the case when all cognitive users have the same rate, i.e., $R_k = R$ for $k \geq 1$. By symmetry the parameters λ_k , β_k and γ_k should be the same for all $k \geq 1$. In this symmetric setup,

one simple observation can be made regarding the optimal number of integer sums L and the coefficient matrix \mathbf{A} .

Lemma 2: For the symmetric many-to-one cognitive interference channel, we need to decode at most two integer sums, $L \leq 2$. Furthermore, the optimal coefficient matrix is one of the following two matrices:

$$\mathbf{A}_1 = \begin{pmatrix} 1 & 0 & \dots & 0 \end{pmatrix} \quad (76)$$

or

$$\mathbf{A}_2 = \begin{pmatrix} c_0 & c & \dots & c \\ 0 & 1 & \dots & 1 \end{pmatrix} \quad (77)$$

for some integer c_0 and nonzero integer c .

Proof: For given $\underline{\lambda}$, $\underline{\beta}$ and $\underline{\gamma}$, to maximize the rate R_k with respect to \mathbf{A} is the same as to minimize the equivalent noise variance $N_0(\ell)$ in (33). We write out $N_0(1)$ for decoding the first equation ($\ell = 1$) with $\beta_k = \beta$, $\lambda_k = \lambda$ and $\gamma_k = \gamma$ for all $k \geq 1$:

$$N_0(1) = \alpha_1^2 + \sum_{k \geq 1} (\alpha_1 b - a_k(1)\beta)^2 \bar{\lambda} P + (\alpha_1 b_0 - a_0(1)\beta_0 - \gamma \sum_{k \geq 1} a_k(1))^2 P$$

The above expression is symmetric on $a_k(1)$ for all $k \geq 1$ hence the minimum is obtained by letting all $a_k(1)$ be the same. It is easy to see that the same argument holds when we induct on ℓ , i.e., for any $\ell \in [1 : L]$, the minimizing $a_k(\ell)$ is the same for $k \geq 1$. Clearly \mathbf{A}_1 and \mathbf{A}_2 satisfy this property.

To see why we need at most two integer sums: the case with \mathbf{A}_1 when the primary decoder decodes one sum is trivial; now consider when it decodes two sums with the coefficients matrix \mathbf{A}_2 . First observe that \mathbf{A}_2 is in the set $\mathcal{A}(2)$, meaning we can solve for \mathbf{t}_0 . Furthermore, there is no need to decode a third sum with $a_k(3)$ all equal for $k \geq 1$, because any other sums of this form can be constructed by using the two sums we already have. We also mention that the coefficient matrix

$$\mathbf{A}_3 = \begin{pmatrix} c_0 & c & \dots & c \\ 1 & 0 & \dots & 0 \end{pmatrix} \quad (78)$$

is also a valid choice and will give the same result as \mathbf{A}_2 . ■

Now we give some numerical results comparing the proposed scheme with the conventional schemes proposed in Section III for the symmetric cognitive many-to-one channels.

Figure 3 shows the achievable rate region for a symmetric cognitive many-to-one channel. The dashed and dot-dash lines are achievable regions with DPC in Proposition 1 and SND at Rx 0 in Proposition 2, respectively. The solid line depicts the rate region using the proposed scheme in Theorem 1. Notice the achievable rates based on the simple conventional schemes in Proposition 1 and 1 are not much better than the trivial time sharing scheme in the multi-user scenario, due to their inherent inefficiencies on interference suppression. On the other hand, the proposed scheme based on structured codes performs interference alignment in the signal level, which gives better interference mitigation ability at the primary receiver. The effect is emphasized more when we study the non-cognitive system in Section V. The outer bound in Figure

3 is obtained by considering the system as a two-user multiple-antenna broadcast channel whose capacity region is known. A brief description to this outer bound is given in Appendix C.

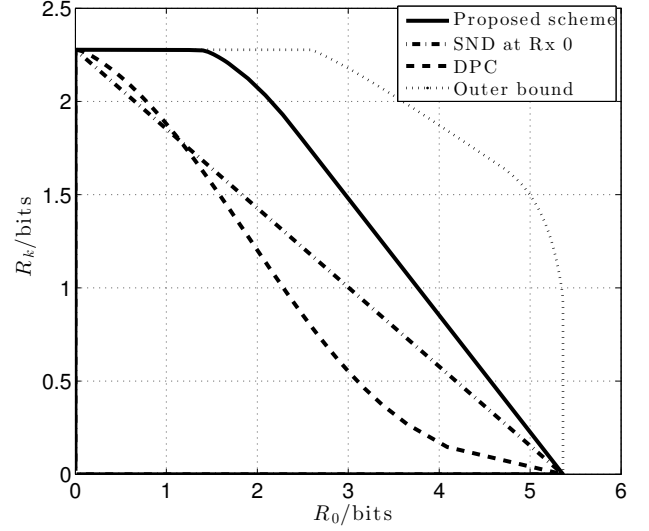


Fig. 3. Achievable rate region for a many-to-one symmetric cognitive many-to-one channel with power $P = 10$, channel gain $b_k = 4$, $h_k = 1.5$ for $k \geq 1$ and $K = 3$ cognitive users. The plot compares the different achievable rates for the cognitive many-to-one channel. The horizontal and vertical axis represents the primary rate R_0 and cognitive rate R_k , $k \geq 1$, respectively.

It is also instructive to study the system performance as a function of the channel gain b . We consider a symmetric channel with h fixed and varying value of b . For different values of b , we maximize the symmetric rate $R_{sym} := \min\{R_0, R\}$ where $R = R_k$ for $k \geq 1$ by choosing optimal \mathbf{A} , $\underline{\lambda}$ and $\underline{\beta}$, i.e.,

$$\max_{\mathbf{A} \in \mathcal{A}(2)} \min_{\substack{\underline{\lambda}, \underline{\beta}}} \left\{ \min_{\ell \in \mathcal{L}_0} r_0(\mathbf{a}_{\ell|1:\ell-1}), \min_{\ell \in \mathcal{L}_k} r_k(\mathbf{a}_{\ell|1:\ell-1}), \max_{\nu_k \in \mathbb{R}} \frac{1}{2} \log^+ \frac{\sigma_k^2}{N_k(\gamma_k)} \right\} \quad (79)$$

where the first term is the rate of the primary user and the minimum of the second and the third term is the rate of cognitive users. Notice $\lambda_k, \beta_k, r_k(\mathbf{a}_{\ell|1:\ell-1})$ are the same for all $k \geq 1$ in this symmetric setup. Figure 4 shows the maximum symmetric rate of different schemes with increasing b .

V. NON-COGNITIVE MANY-TO-ONE CHANNELS

As an interesting special case of the cognitive many-to-one channel, in this section we will study the non-cognitive many-to-one channels where user $1, \dots, K$ do not have access to the message W_0 of User 0. The many-to-one interference channel has also been studied, for example, in [9], where several constant-gap results are obtained. Using the coding scheme introduced here, we are able to give some refined result to this channel in some special cases.

It is straightforward to extend the coding scheme of the cognitive channel to the non-cognitive channel by letting users $1, \dots, K$ not split the power for the message W_0 but to transmit their own messages only. The achievable rates are the same as

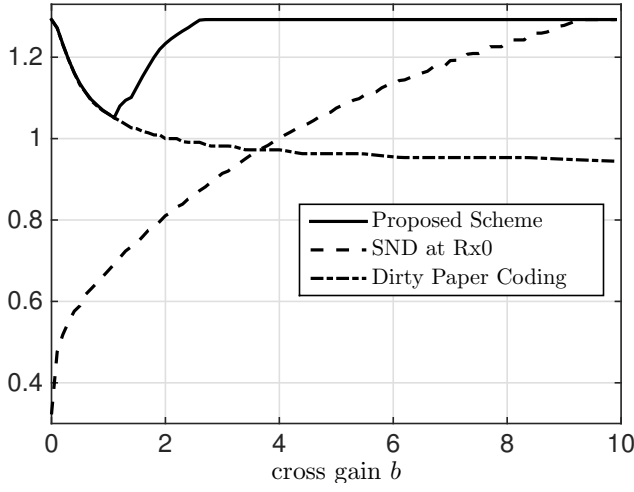


Fig. 4. The maximum symmetric rates R_{sym} of different schemes for a many-to-one cognitive interference network with power $P = 5$ and $K = 3$ cognitive users where $R_k = R$ for $k \geq 1$. We set $h = 1$ and vary the cross channel gain b in the interval $[0 : 10]$. Notice the maximum symmetric rate is upper bounded by $\frac{1}{2} \log(1 + h^2 P)$. We see the proposed scheme performs better than the other two schemes in general. When the interference becomes larger, the proposed scheme quickly attains the maximum symmetric rate. The joint decoding method approaches the maximum symmetric rate much slower, since it requires the cross channel gain to be sufficiently large such that the primary decoder can (nonuniquely) decode all the messages of the cognitive users. The dirty paper coding approach cannot attain the maximum symmetric rate since the primary decoder treats interference as noise.

in Theorem 1 by setting all power splitting parameters λ_k to be zero and γ_k to be zero because \mathbf{x}_0 will not be interference to cognitive users. Although it is a straightforward exercise to write out the achievable rates, we still state the result formally here.

Theorem 2: For any given positive numbers $\underline{\beta}$ and coefficient matrix $\mathbf{A} \in \mathcal{A}(L)$ in (36) with $L \in [1 : K + 1]$, define $\mathcal{L}_k := \{\ell \in [1 : L] | a_k(\ell) \neq 0\}$. If $r_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\lambda}, \underline{\beta}, \underline{\gamma}) > 0$ for all $\ell \in \mathcal{L}_k$, $k \in [0 : K]$, then the following rate is achievable for the many-to-one interference channel

$$R_0 \leq \min_{\ell \in \mathcal{L}_0} \tilde{r}_0(\mathbf{a}_{\ell|1:\ell-1}, \underline{\beta}) \quad (80a)$$

$$R_k \leq \min \left\{ \frac{1}{2} \log(1 + h_k^2 P), \min_{\ell \in \mathcal{L}_k} \tilde{r}_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\beta}) \right\} \quad (80b)$$

for $k \in [1 : K]$ with

$$\tilde{r}_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\beta}) := \max_{\alpha_1, \dots, \alpha_\ell \in \mathbb{R}} \frac{1}{2} \log^+ \left(\frac{\beta_k^2 P}{\tilde{N}_0(\ell)} \right) \quad (81)$$

where $\tilde{N}_0(\ell)$ is defined as

$$\begin{aligned} \tilde{N}_0(\ell) := & \alpha_\ell^2 + \sum_{k \geq 1} \left(\alpha_\ell b_k - a_k(\ell) \beta_k - \sum_{j=1}^{\ell-1} \alpha_j a_k(j) \beta_k \right)^2 P \\ & + \left(\alpha_\ell - a_0(\ell) \beta_0 - \sum_{j=1}^{\ell-1} \alpha_j a_0(j) \beta_0 \right)^2 P. \end{aligned} \quad (82)$$

Proof: The proof of this result is almost the same as the proof of Theorem 1 in Section IV-D. The only change in this proof is that the user $1, \dots, K$ do not split the power to

transmit for the primary user and all γ_k are set to be zero since \mathbf{x}_0 will not act as interference to cognitive receivers. We will use lattice codes described in Section IV-A but adjust the code construction. Given positive numbers $\underline{\beta}$ and a simultaneously good fine lattice Λ , we choose $K + 1$ simultaneously good lattices such that $\Lambda_k^s \subseteq \Lambda_k$ with second moments $\sigma^2(\Lambda_k^s) = \beta_k^2 P$ for all $k \in [0 : K]$.

Each user forms the transmitted signal as

$$\mathbf{x}_k = \left[\frac{\mathbf{t}_k}{\beta_k} + \mathbf{d}_k \right] \bmod \Lambda_k^s / \beta_k, \quad k \in [0 : K] \quad (83)$$

The analysis of the decoding procedure at all receivers is the same as in Section IV-D. User 0 decodes integer sums to recover \mathbf{t}_0 and other users decode their message \mathbf{t}_k directly from the channel output using lattice decoding. In fact, the expression $\tilde{r}_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\beta})$ in (81) is the same as $r_k(\mathbf{a}_{\ell|1:\ell-1}, \underline{\lambda}, \underline{\beta}, \underline{\gamma})$ in (32) by letting $\lambda_k = \gamma_k = 0$ in the later expression. Furthermore we have

$$\max_{\nu_k \in \mathbb{R}} \frac{1}{2} \log \frac{\sigma_k^2}{N_k(\gamma_k = 0)} = \frac{1}{2} \log(1 + h_k^2 P) \quad (84)$$

for any choice of $\beta_k, k \geq 1$. ■

For a simple symmetric example, we compare the achievable rate region of the cognitive many-to-one channel (Theorem 1) with the achievable rate region of the non-cognitive many-to-one channel (Theorem 2) in Figure 5. The parameters are the same for both channel. This shows the usefulness of the cognitive messages in the system.

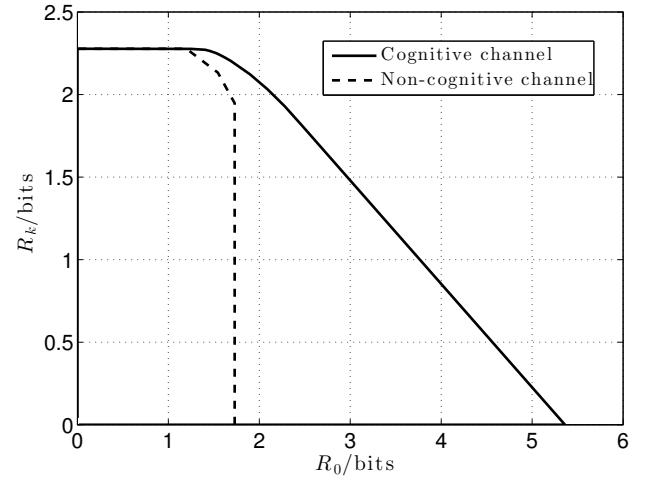


Fig. 5. A many-to-one symmetric interference channel with power $P = 10$, channel gain $b_k = 4$, $h_k = 1.5$ for $k \geq 1$ and $K = 3$ cognitive users. This plot compares the different achievable rate regions for the cognitive and non-cognitive channel. The horizontal and vertical axis represents the primary rate R_0 and cognitive rate $R_k, k \geq 1$, respectively. The rate region for the cognitive channel given by Theorem 1 is plotted in solid line. The dashed line gives the achievable rate region in Theorem 2 for the non-cognitive many-to-one channel.

A. Capacity Results for Non-cognitive Symmetric Channels

Now we consider a symmetric non-cognitive many-to-one channel where $b_k = b$ and $h_k = h$ for $k \geq 1$. In [9], an approximate capacity result is established within a gap of $(3K + 3)(1 + \log(K + 1))$ bits per user for any channel gain.

In this section we will give refined results for the symmetric many-to-one channel. The reason we restrict ourselves to the symmetric case is that, for general channel gains the optimization problem involving the coefficient matrix \mathbf{A} is analytically intractable as discussed in Section IV-C, hence it is also difficult to give explicit expressions for achievable rates. But for the symmetric many-to-one channel we are able to give a constant gap result as well as a capacity result when the interference is strong. First notice that the optimal form of the coefficient matrix for the cognitive symmetric channel given in Lemma 2 also applies in this non-cognitive symmetric setting.

Theorem 3: Consider a symmetric (non-cognitive) many-to-one interference channel with $K + 1$ users. If $|b| \geq |h| \lceil \sqrt{P} \rceil$, then each user is less than 0.5 bit from the capacity for any number of users. Furthermore, if $|b| \geq \sqrt{\frac{(1+P)(1+h^2P)}{P}}$, each user can achieve the capacity, i.e., $R_0 = \frac{1}{2} \log(1+P)$ and $R_k = \frac{1}{2} \log(1+h^2P)$ for all $k \geq 1$.

Proof: For the symmetric non-cognitive many-to-one channel, we have the following trivial capacity bound

$$R_0 \leq \frac{1}{2} \log(1+P) \quad (85)$$

$$R_k \leq \frac{1}{2} \log(1+h^2P). \quad (86)$$

To show the constant gap result, we choose the coefficients matrix of the two sums to be

$$\mathbf{A} = \begin{pmatrix} 1 & c & \dots & c \\ 0 & 1 & \dots & 1 \end{pmatrix} \quad (87)$$

for some nonzero integer c . Furthermore we choose $\beta_0 = 1$ and $\beta_k = b/c$ for all $k \geq 1$. In Appendix D we use Theorem 2 to show the following rates are achievable:

$$R_0 = \frac{1}{2} \log^+ P$$

$$R_k = \min \left\{ \frac{1}{2} \log^+ \frac{b^2 P}{c^2}, \frac{1}{2} \log^+ b^2, \frac{1}{2} \log(1+h^2P) \right\}.$$

If $|b| \geq |h| \lceil \sqrt{P} \rceil$, choosing $c = \lceil \sqrt{P} \rceil$ will ensure $R_k \geq \frac{1}{2} \log^+ h^2 P$.

Notice that for $P \leq 1$, then $\frac{1}{2} \log(1+P) \leq 0.5$ hence the claim is vacuously true. For $P \geq 1$, we have

$$\frac{1}{2} \log(1+P) - R_0 \leq \frac{1}{2} \log \frac{1+P}{P} \leq \frac{1}{2} \log 2 = 0.5 \text{ bit}$$

With the same argument we have

$$\frac{1}{2} \log(1+h^2P) - R_k \leq 0.5 \text{ bit} \quad (88)$$

To show the capacity result, we set $\beta_0 = 1$ and $\beta_k = \beta$ for all $k \geq 1$. The receiver 0 decodes two sums with the coefficients matrix

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & \dots & 1 \\ 1 & 0 & \dots & 0 \end{pmatrix}. \quad (89)$$

The achievable rates using Theorem 2 is shown in Appendix D to be

$$R_0 = \frac{1}{2} \log(1+P) \quad (90)$$

$$R_k = \min \left\{ \frac{1}{2} \log \left(\frac{Pb^2}{1+P} \right), \frac{1}{2} \log(1+h^2P) \right\}. \quad (91)$$

The inequality

$$\frac{Pb^2}{1+P} \geq 1+h^2P \quad (92)$$

is satisfied if it holds that

$$b^2 \geq \frac{(1+P)(1+h^2P)}{P}. \quad (93)$$

This completes the proof. \blacksquare

Comparing to the constant gap result in [9], our result only concerns a special class of many-to-one channel, but gives a gap which does not depend on the number of users K . We also point out that in [24], a K -user symmetric interference channel is studied where it was shown that if the cross channel gain h satisfies $|h| \geq \sqrt{\frac{(1+P)^2}{P}}$, then every user achieves the capacity $\frac{1}{2} \log(1+P)$. This result is very similar to our result obtained here and is actually obtained using the same coding technique.

APPENDIX A

DERIVATIONS IN THE PROOF OF THEOREM 1

We give the proof for the claim made in Section IV-D that we could form the equivalent channel

$$\tilde{\mathbf{y}}_0^{(\ell)} = \tilde{\mathbf{z}}_0(\ell) + \sum_{k \geq 0} a_k(\ell) \tilde{\mathbf{t}}_k$$

with $\tilde{\mathbf{z}}_0(\ell)$ defined in (67) when the primary decoder decodes the ℓ -th integer sum $\sum_{k \geq 0} a_k(\ell) \tilde{\mathbf{t}}_k$ for $\ell \geq 2$.

We first show the base case for $\ell = 2$. Since $\sum_{k \geq 0} a_k(1) \tilde{\mathbf{t}}_k$ is decoded, the equivalent noise $\tilde{\mathbf{z}}_0(1)$ in Eqn. (58) can be inferred from $\tilde{\mathbf{y}}_0$. Given α_{20}, α_{21} we form the following with \mathbf{y}_0 in (53) and $\tilde{\mathbf{z}}_0(1)$

$$\begin{aligned} \tilde{\mathbf{y}}_0^{(2)} &:= \alpha_{20} \mathbf{y}_0 + \alpha_{21} \tilde{\mathbf{z}}_0(1) \\ &= (\alpha_{20} + \alpha_{21} \alpha_1) \mathbf{z}_0 \\ &\quad + \sum_{k \geq 1} ((\alpha_{20} + \alpha_{21} \alpha_1) b_k - \alpha_{21} a_k(1) \beta_k) \hat{\mathbf{x}}_k \\ &\quad + ((\alpha_{20} + \alpha_{21} \alpha_1) b_0 - \alpha_{21} a_0(1) \beta_0 - \alpha_{21} g(1)) \mathbf{x}_0 \\ &= \alpha'_2 \mathbf{z}_0 + \sum_{k \geq 1} (\alpha'_2 b_k - \alpha'_1 a_k(1) \beta_k) \hat{\mathbf{x}}_k \\ &\quad + (\alpha'_2 b_0 - \alpha'_1 a_0(1) \beta_0 - \alpha'_1 g(1)) \mathbf{x}_0 \end{aligned}$$

by defining $\alpha'_1 := \alpha_{21}$ and $\alpha'_2 := \alpha_{20} + \alpha_{21} \alpha_1$. Now following the same step for deriving $\tilde{\mathbf{y}}_0^{(1)}$ in (57), we can rewrite $\tilde{\mathbf{y}}_0^{(2)}$ as

$$\tilde{\mathbf{y}}_0^{(2)} = \sum_{k \geq 0} a_k(2) \tilde{\mathbf{t}}_k + \tilde{\mathbf{z}}_0(2) \quad (94)$$

with

$$\begin{aligned} \tilde{\mathbf{z}}_0(2) &:= \alpha'_2 \mathbf{z}_0 + \sum_{k \geq 1} (\alpha'_2 b_k - a_k(2) \beta_k - \alpha'_1 a_k(1) \beta_k) \hat{\mathbf{x}}_k \\ &\quad + (\alpha'_2 b_0 - a_0(2) \beta_0 - \alpha'_1 a_0(1) \beta_0 - g(2)) \mathbf{x}_0 \end{aligned}$$

This establishes the base case by identifying $\alpha'_i = \alpha_i$ for $i = 1, 2$.

Now assume the expression (67) is true for $\ell - 1$ ($\ell \geq 3$) and we have inferred $\tilde{\mathbf{z}}_0(m)$ from $\tilde{\mathbf{y}}_0^{(m)}$ using the decoded sum $\sum_{k \geq 0} a_k(m) \tilde{\mathbf{t}}_k$ for all $m \leq 1, \dots, \ell - 1$, we will form $\tilde{\mathbf{y}}_0^{(\ell)}$ with ℓ numbers $\alpha_{\ell 0}, \dots, \alpha_{\ell \ell-1}$ as

$$\begin{aligned} \tilde{\mathbf{y}}_0^{(\ell)} &:= \alpha_{\ell 0} \mathbf{y}_0 + \sum_{m=1}^{\ell-1} \alpha_{\ell m} \tilde{\mathbf{z}}_0(m) \\ &= \alpha'_\ell \mathbf{z}_0 + \sum_{k \geq 1} (\alpha'_\ell b_k - \beta_k C_{\ell-1}(k)) \hat{\mathbf{x}}_k \\ &\quad + \left(\alpha'_\ell b_0 - \beta_0 C_{\ell-1}(0) - \sum_{m=1}^{\ell-1} \alpha_{\ell m} g(m) \right) \mathbf{x}_0 \end{aligned}$$

with

$$\alpha'_\ell := \alpha_{\ell 0} + \sum_{m=1}^{\ell-1} \alpha_{\ell m} \alpha_m \quad (95)$$

$$C_{\ell-1}(k) := \sum_{m=1}^{\ell-1} \alpha_{\ell m} \left(a_k(m) + \sum_{j=1}^{m-1} \alpha_j a_k(j) \right). \quad (96)$$

Algebraic manipulations allow us to rewrite $C_{\ell-1}(k)$ as

$$C_{\ell-1}(k) = \sum_{m=1}^{\ell-1} \left(\alpha_{\ell m} + \alpha_m \sum_{j=m+1}^{\ell-1} \alpha_{\ell j} \right) a_k(m) \quad (97)$$

$$= \sum_{m=1}^{\ell-1} \alpha'_m a_k(m) \quad (98)$$

by defining $\alpha'_m := \alpha_{\ell m} + \alpha_m \sum_{j=m+1}^{\ell-1} \alpha_{\ell j}$ for $m = 1, \dots, \ell - 1$. Substituting the above into $\tilde{\mathbf{y}}_0^{(\ell)}$ we get

$$\begin{aligned} \tilde{\mathbf{y}}_0^{(\ell)} &= \alpha'_\ell \mathbf{z}_0 + \sum_{k \geq 1} \left(\alpha'_\ell b_k - \beta_k \sum_{m=1}^{\ell-1} \alpha'_m a_k(m) \right) \hat{\mathbf{x}}_k \\ &\quad + \left(\alpha'_\ell b_0 - \beta_0 \sum_{m=1}^{\ell-1} \alpha'_m a_0(m) - \sum_{m=1}^{\ell-1} \alpha_{\ell m} g(m) \right) \mathbf{x}_0. \end{aligned}$$

Together with the definition of $g(m)$ in (35) and some algebra we can show

$$\sum_{m=1}^{\ell-1} \alpha_{\ell m} g(m) = \sum_{k=1}^K \gamma_k C_{\ell-1}(k) \quad (99)$$

$$= \sum_{k=1}^K \left(\sum_{m=1}^{\ell-1} \alpha'_m a_k(m) \right) \gamma_k. \quad (100)$$

Finally using the same steps for deriving $\tilde{\mathbf{y}}_0^{(1)}$ in (57) and identifying $\alpha'_m = \alpha_m$ for $m = 1, \dots, \ell$, it is easy to see that we have

$$\tilde{\mathbf{y}}_0^{(\ell)} = \sum_{k \geq 0} a_k(\ell) \tilde{\mathbf{t}}_k + \tilde{\mathbf{z}}_0(\ell) \quad (101)$$

with $\tilde{\mathbf{z}}_0(\ell)$ claimed in (67).

APPENDIX B PROOF OF PROPOSITION 3

For any given set of parameters $\{\alpha_j, j \in [1 : \ell]\}$ in the expression $N_0(\ell)$ in (42), we can always find another set of parameters $\{\alpha'_j, j \in [1 : \ell]\}$ and a set of vectors $\{\mathbf{u}_j, j \in [1 : \ell]\}$, such that

$$\alpha_\ell \mathbf{h} + \sum_{j=1}^{\ell-1} \alpha_j \tilde{\mathbf{a}}_j = \sum_{j=1}^{\ell} \alpha'_j \mathbf{u}_j \quad (102)$$

as long as the two sets of vectors, $\{\mathbf{h}, \tilde{\mathbf{a}}_j, j \in [1 : \ell - 1]\}$ and $\{\mathbf{u}_j, j \in [1 : \ell]\}$ span the same subspace. If we choose an appropriate set of basis vectors $\{\mathbf{u}_j\}$, the minimization problem of $N_0(\ell)$ can be equivalently formulated with the set $\{\mathbf{u}_j\}$ and new parameters $\{\alpha'_j\}$ where the optimal $\{\alpha'_j\}$ have simple solutions. Notice that $\{\mathbf{u}_j, j \in [1 : \ell]\}$ in Eqn. (45) are obtained by performing the Gram-Schmidt procedure on the set $\{\mathbf{h}, \tilde{\mathbf{a}}_j, j \in [1 : \ell - 1]\}$. Hence the set $\{\mathbf{u}_j, j \in [1 : \ell]\}$ contains orthogonal vectors and spans the same subspace as the set $\{\mathbf{h}, \tilde{\mathbf{a}}_j, j \in [1 : \ell - 1]\}$ does. For any $\ell \geq 1$, the expression $N_0(\ell)$ in (42) can be equivalently rewritten as

$$N_0(\ell) = \alpha_\ell'^2 + \left\| \sum_{j=1}^{\ell} \alpha'_j \mathbf{u}_j - \tilde{\mathbf{a}}_\ell \right\|^2 P \quad (103)$$

with $\{\mathbf{u}_j\}$ defined above and some $\{\alpha'_j\}$. Due to the orthogonality of vectors $\{\mathbf{u}_j\}$, we have the following simple optimal solutions for $\{\alpha'_j\}$ which minimize $N_0(\ell)$:

$$\alpha_j'^* = \frac{\tilde{\mathbf{a}}_\ell^T \mathbf{u}_j}{\|\mathbf{u}_j\|^2}, \quad j \in [1 : \ell - 1] \quad (104)$$

$$\alpha_\ell'^* = \frac{P \tilde{\mathbf{a}}_\ell^T \mathbf{u}_\ell}{P \|\mathbf{u}_\ell\|^2 + 1}. \quad (105)$$

Substituting them back to $N_0(\ell)$ in (103) we have

$$\begin{aligned} N_0(\ell) &= P \|\tilde{\mathbf{a}}_\ell\|^2 - \sum_{j=1}^{\ell-1} \frac{(\tilde{\mathbf{a}}_\ell^T \mathbf{u}_j)^2 P}{\|\mathbf{u}_j\|^2} - \frac{P^2 (\mathbf{u}_\ell^T \tilde{\mathbf{a}}_\ell)^2}{1 + P \|\mathbf{u}_\ell\|^2} \\ &= P \tilde{\mathbf{a}}_\ell^T \left(\mathbf{I} - \sum_{j=1}^{\ell-1} \frac{\mathbf{u}_j \mathbf{u}_j^T}{\|\mathbf{u}_j\|^2} - \frac{(\mathbf{u}_\ell \mathbf{u}_\ell^T) P}{1 + P \|\mathbf{u}_\ell\|^2} \right) \tilde{\mathbf{a}}_\ell \\ &= P \mathbf{a}(\ell)^T \mathbf{B}_\ell \mathbf{a}(\ell) \end{aligned}$$

with \mathbf{B}_ℓ given in (47). As we discussed before, maximizing $r_k(\mathbf{a}_{\ell[1:\ell-1]})$ is equivalent to minimizing $N_0(\ell)$ and the optimal coefficients $\mathbf{a}(\ell), \ell \in [1 : L]$ are the same for all users. This proves the claim.

APPENDIX C AN OUTER BOUND ON THE CAPACITY REGION

In this section we give a simple outer bound on the capacity region of the cognitive many-to-one channel, which is used for the numerical evaluation in Figure 3, Section IV-E. Notice that if we allow all transmitters $k = 0, \dots, K$ to cooperate, and allow the cognitive receivers $k = 1, \dots, K$ to cooperate, then the system can be seen as a 2-user broadcast channel where the transmitter has $K + 1$ antennas. The two users are the primary receiver and the aggregation of all cognitive receivers with K

antennas. Obviously the capacity region of this resulting 2-user MIMO broadcast channel will be a valid outer bound on the capacity region of the cognitive many-to-one channel. The capacity region \mathcal{C}_{BC} of the broadcast channel is given by (see [15, Ch. 9] for example)

$$\mathcal{C}_{BC} = \mathcal{R}_1 \cup \mathcal{R}_2 \quad (106)$$

where \mathcal{R}_1 is defined as

$$R_1 \leq \frac{1}{2} \log \frac{|\mathbf{H}_1(\mathbf{K}_1 + \mathbf{K}_2)\mathbf{H}_1^T + \mathbf{I}|}{|\mathbf{H}_1\mathbf{K}_2\mathbf{H}_2^T + \mathbf{I}|} \quad (107)$$

$$R_2 \leq \frac{1}{2} \log |\mathbf{H}_2\mathbf{K}_2\mathbf{G}_2^T + \mathbf{I}| \quad (108)$$

and \mathcal{R}_2 defined similarly with all subscripts 1 and 2 in \mathcal{R}_1 swapped. The channel matrices $\mathbf{H}_1 \in \mathbb{R}^{1 \times (K+1)}$ and $\mathbf{H}_2 \in \mathbb{R}^{K \times (K+1)}$ are defined as

$$\mathbf{H}_1 = [1 \quad b_1 \quad \dots \quad b_K] \quad (109)$$

$$\mathbf{H}_2 = \begin{bmatrix} 0 & h_1 & 0 & \dots & 0 \\ 0 & 0 & h_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & h_K \end{bmatrix} \quad (110)$$

where \mathbf{H}_1 denotes the channel from the aggregated transmitters to the primary receiver and \mathbf{H}_2 denotes the channel to all cognitive receivers. The variables $\mathbf{K}_1, \mathbf{K}_2 \in \mathbb{R}^{(K+1) \times (K+1)}$ should satisfy the condition

$$\text{tr}(\mathbf{K}_1 + \mathbf{K}_2) \leq (K+1)P \quad (111)$$

which represents the power constraint for the corresponding broadcast channel³. As explained in [15, Ch. 9], the problem of finding the region \mathcal{C}_{BC} can be rewritten as convex optimization problems which are readily solvable using standard convex optimization tools.

APPENDIX D

DERIVATIONS IN THE PROOF OF THEOREM 3

We give detailed derivations of the achievable rates in Theorem 3 with two chosen coefficient matrices.

When the primary user decodes the first equation ($\ell = 1$) in a symmetric channel, the expression (82) for the variance of the equivalent noise simplifies to (denoting $\beta_k = \beta$ for $k \geq 1$)

$$\tilde{N}_0(1) = \bar{\alpha}_1^2 + K(\bar{\alpha}_1 b - a_k(1)\beta)^2 P + (\bar{\alpha}_1 - a_0(1)\beta_0)^2 P. \quad (112)$$

For decoding the second integer sum, the variance of the equivalent noise (82) is given as

$$\begin{aligned} \tilde{N}_0(2) = & \alpha_2^2 + K(\alpha_2 b - a_k(2)\beta - \alpha_1 a_k(1)\beta)^2 P \\ & + (\alpha_2 - a_0(2)\beta_0 - \alpha_1 a_0(1)\beta_0)^2 P. \end{aligned} \quad (113)$$

We first evaluate the achievable rate for the coefficient matrix in (87). We choose $\beta_0 = 1$ and $\beta = b/c$. Using Theorem 2, substituting $\mathbf{a}(1) = [1, c, \dots, c]$ and the optimal

³Since each transmitter has its individual power constraint, we could give a slightly tighter outer bound by imposing a per-antenna power constraint. Namely the matrices $\mathbf{K}_1, \mathbf{K}_2$ should satisfy $(\mathbf{K}_1 + \mathbf{K}_2)_{ii} \leq P$ for $i \in [1 : K+1]$ where $(\mathbf{X})_{ii}$ denotes the (i, i) entry of matrix \mathbf{X} . However this is not the focus of this paper and we will not pursue it here.

$\bar{\alpha}_1^* = 1 - \frac{1}{P(Kb^2+1)}$ into (112) will give us a rate constraint on R_0

$$\tilde{r}_0(\mathbf{a}_1, \underline{\beta}) = \frac{1}{2} \log^+ \left(\frac{1}{1 + Kb^2} + P \right) > \frac{1}{2} \log^+ P$$

$$\tilde{r}_k(\mathbf{a}_1, \underline{\beta}) = \frac{1}{2} \log^+ \left(\frac{b^2 P(Kb^2 P + P + 1)}{c^2(Kb^2 P + P)} \right) > \frac{1}{2} \log^+ \frac{b^2 P}{c^2}.$$

Notice here we have replaced the achievable rates with smaller values to make the result simple. We will do the same in the following derivation.

For decoding the second sum with coefficients $\mathbf{a}(2) = [0, 1, \dots, 1]$, we use Theorem 2 and (113) to obtain rate constraints for R_k

$$\tilde{r}_k(\mathbf{a}_{2|1}, \underline{\beta}) = \frac{1}{2} \log^+ \left(b^2 + \frac{1}{K} \right) > \frac{1}{2} \log^+ b^2 \quad (114)$$

with the optimal $\alpha_1^* = \frac{-b^2 K}{c(Kb^2+1)}$ and $\alpha_2^* = 0$. Notice that $\mathbf{a}_0(1) = 0$ hence decoding this sum will not impose any rate constraint on R_0 . Therefore we omit the expression $\tilde{r}_0(\mathbf{a}_{2|1}, \underline{\beta})$. Combining the results above with Theorem 2 we get the claimed rates in the proof of Theorem 3.

Now we evaluate the achievable rate for the coefficient matrix in (89). We substitute $\beta_0 = 1, \beta_k = \beta$ for any β and $\mathbf{a}(1) = [0, 1, \dots, 1]$ in (112) with the optimal $\bar{\alpha}_1^* = \frac{Kb\beta P}{Kb^2 P + P + 1}$. Notice again R_0 is not constrained by decoding this sum hence we only have the constraint on R_k as

$$\tilde{r}_k(\mathbf{a}_1, \underline{\beta}) = \frac{1}{2} \log^+ \left(\frac{1}{K} + \frac{P}{1+P} b^2 \right) > \frac{1}{2} \log^+ \frac{Pb^2}{1+P}.$$

For the second decoding, using $\mathbf{a}(2) = [1, 0, \dots, 0]$ in (113) gives

$$\tilde{r}_0(\mathbf{a}_{2|1}, \underline{\beta}) = \frac{1}{2} \log(1 + P) \quad (115)$$

with the optimal scaling factors $\alpha_1^* = \frac{bP}{\beta(P+1)}$ and $\alpha_2^* = \frac{P}{P+1}$. Combining the achievable rates above with Theorem 2 gives the claimed result.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper.

REFERENCES

- [1] N. Devroye, P. Mitran, and V. Tarokh, "Achievable rates in cognitive radio channels," *Information Theory, IEEE Transactions on*, vol. 52, pp. 1813–1827, May 2006.
- [2] I. Marić, A. Goldsmith, G. Kramer, and S. Shamai (Shitz), "On the capacity of interference channels with one cooperating transmitter," *European Transactions on Telecommunications*, vol. 19, pp. 405–420, 2008.
- [3] A. Jovicic and P. Viswanath, "Cognitive radio: An information-theoretic perspective," *Information Theory, IEEE Transactions on*, vol. 55, pp. 3945–3958, 2009.
- [4] S. Rini, D. Tuninetti, and N. Devroye, "Inner and outer bounds for the Gaussian cognitive interference channel and new capacity results," *Information Theory, IEEE Transactions on*, vol. 58, pp. 820–848, 2012.
- [5] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," *Information Theory, IEEE Transactions on*, vol. 57, pp. 6463–6486, 2011.
- [6] J. Zhu and M. Gastpar, "Asymmetric compute-and-forward with CSIT," in *International Zurich Seminar on Communications*, 2014.

- [7] K. G. Nagananda, P. Mohapatra, C. R. Murthy, and S. Kishore, "Multiuser cognitive radio networks: an information-theoretic perspective," *International Journal of Advances in Engineering Sciences and Applied Mathematics*, vol. 5, no. 1, pp. 43–65, Mar. 2013.
- [8] D. Maamari, D. Tuninetti, and N. Devroye, "Approximate sum-capacity of k-user cognitive interference channels with cumulative message sharing," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 3, pp. 654–666, Mar. 2014.
- [9] G. Bresler, A. Parekh, and D. N. C. Tse, "The approximate capacity of the many-to-one and one-to-many Gaussian interference channels," *Information Theory, IEEE Transactions on*, vol. 56, pp. 4566–4592, 2010.
- [10] W. Nam, S.-Y. Chung, and Y. H. Lee, "Capacity of the Gaussian two-way relay channel to within 1/2 bit," *Information Theory, IEEE Transactions on*, vol. 56, no. 11, pp. 5488–5494, 2010.
- [11] M. Wilson, K. Narayanan, H. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bidirectional relaying," *Information Theory, IEEE Transactions on*, vol. 56, no. 11, 2010.
- [12] O. Ordentlich, U. Erez, and B. Nazer, "The approximate sum capacity of the symmetric Gaussian K-user interference channel," *arXiv:1206.0197 [cs, math]*, Jun. 2012.
- [13] J. Zhan, B. Nazer, U. Erez, and M. Gastpar, "Integer-forcing linear receivers," arXiv e-print, Mar. 2010. [Online]. Available: <http://arxiv.org/abs/1003.5966>
- [14] W. Wu, S. Vishwanath, and A. Arapostathis, "Capacity of a class of cognitive radio channels: Interference channels with degraded message sets," *Information Theory, IEEE Transactions on*, vol. 53, pp. 4391–4399, 2007.
- [15] A. El Gamal and Y. H. Kim, *Network information theory*. Cambridge University Press, 2011.
- [16] U. Erez, S. Litsyn, and R. Zamir, "Lattices which are good for (almost) everything," *Information Theory, IEEE Transactions on*, vol. 51, pp. 3401–3416, 2005.
- [17] U. Erez and R. Zamir, "Achieving $1/2 \log(1 + \text{SNR})$ on the AWGN channel with lattice encoding and decoding," *Information Theory, IEEE Transactions on*, vol. 50, pp. 2293–2314, 2004.
- [18] G. Poltyrev, "On coding without restrictions for the AWGN channel," *Information Theory, IEEE Transactions on*, vol. 40, pp. 409–417, 1994.
- [19] W. Nam, S. Y. Chung, and Y. H. Lee, "Nested lattice codes for Gaussian relay networks with interference," *Information Theory, IEEE Transactions on*, vol. 57, pp. 7733–7745, 2011.
- [20] R. Zamir, S. Shamai, and U. Erez, "Nested linear/lattice codes for structured multiterminal binning," *Information Theory, IEEE Transactions on*, vol. 48, no. 6, pp. 1250–1276, 2002.
- [21] B. Nazer, "Successive compute-and-forward," in *International Zurich Seminar on Communications*, 2012, p. 103.
- [22] S. S. Bidokhti, V. M. Prabhakaran, and S. Diggavi, "Is non-unique decoding necessary?" in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, 2012, p. 398402.
- [23] S. Sahaee and M. Gastpar, "Compute-and-forward: Finding the best equation," in *52nd Annual Allerton Conference on Communication, Control, and Computing, Champaign, Illinois, USA*, 2014.
- [24] S. Sridharan, A. Jafarian, S. Vishwanath, and S. Jafar, "Capacity of symmetric K-user Gaussian very strong interference channels," in *IEEE Global Telecommunications Conference*, 2008.

Michael Gastpar received the Dipl. El.-Ing. degree from ETH Zürich, in 1997, the M.S. degree from the University of Illinois at Urbana-Champaign, Urbana, IL, in 1999, and the Doctorat ès Science degree from Ecole Polytechnique Fédérale (EPFL), Lausanne, Switzerland, in 2002, all in electrical engineering. He was also a student in engineering and philosophy at the Universities of Edinburgh and Lausanne.

He is a Professor in the School of Computer and Communication Sciences, Ecole Polytechnique Fédérale (EPFL), Lausanne, Switzerland. He held tenured professor positions at the University of California, Berkeley, and at Delft University of Technology, The Netherlands. He was a Researcher with the Mathematics of Communications Department, Bell Labs, Lucent Technologies, Murray Hill, NJ. His research interests are in network information theory and related coding and signal processing techniques, with applications to sensor networks and neuroscience.

Dr. Gastpar received the 2002 EPFL Best Thesis Award, the NSF CAREER Award in 2004, the Okawa Foundation Research Grant in 2008, the ERC Starting Grant in 2010, and the IEEE Communications Society and Information Theory Society Joint Paper Award in 2013. He was an Information Theory Society Distinguished Lecturer (2009–2011), an Associate Editor for Shannon Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY (2008–2011), and he has served as Technical Program Committee Co-Chair for the 2010 International Symposium on Information Theory, Austin, TX.

Jingge Zhu is a Ph.D. student in the School of Computer and Communication Sciences, Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland. He received the B.S. degree and M.S. degree in electrical engineering from Shanghai Jiao Tong University, Shanghai, China, in 2008 and 2011, respectively. He also received the Dipl.-Ing. degree in technische Informatik from Technische Universität Berlin, Berlin, Germany in 2011. His research interests include information theory with applications in communication systems.

Mr. Zhu is the recipient of the IEEE Heinrich Hertz Award for Best Communications Letters in 2013.